数学类专业学习辅导丛书

Guidance Series for Mathematics Majors

近世代数三百题

Jinshi Daishu Sanbai Ti

冯克勤　章　璞



高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容简介

本书为近世代数的教学提供了丰富的例子，内容包括群论、环论、域论和 Galois 理论。全书包含了 500 多个习题（包括一大题中若干小题）的解答；有近三分之一或更多的题目对初学者是较难的；有的题目是很难的（例如，华罗庚恒等式等题，在一般的书中也很难找到解答）。为帮助学生回顾所学内容，在每一节前加了“知识要点”。

本书可作为数学系本科生和研究生及其他相关专业学生的教学参考书和课外读物。

图书在版编目（CIP）数据

近世代数三百题/冯克勤，章璞．—北京：高等教育出版社，2010.1
ISBN 978-7-04-028324-2

Ⅰ．近… Ⅱ．①冯… ②章… Ⅲ．抽象代数-习题
Ⅳ．0153-44

中国版本图书馆 CIP 数据核字（2009）第 221324 号

策划编辑 杨 波　　责任编辑 张耀明　　封面设计 赵 阳
版式设计 史新薇　　责任校对 王 超　　责任印制 朱学忠

出版发行 高等教育出版社　　购书热线 010-58581118
社 址 北京市西城区德外大街 4 号　　咨询电话 400-810-0598
邮政编码 100120　　网 址 http://www.hep.edu.cn
总 机 010-58581000　　http://www.hep.com.cn
网上订购 http://www.landraco.com
经 销 蓝色畅想图书发行有限公司　　http://www.landraco.com.cn
印 刷 北京联兴盛业印刷股份有限公司　　畅想教育 http://www.widedu.com

开 本 787×960 1/16　　版 次 2010 年 1 月第 1 版
印 张 12.25　　印 次 2010 年 1 月第 1 次印刷
字 数 220 000　　定 价 16.20 元

物料号 28324-00

前　言

由冯克勤、李尚志、查建国、章璞编写的《近世代数引论》, 历经三版反复修改, 作为数学系本科生教材使用已二十余年。这本教材有不少较难的习题。十几年前, 我们在教学过程中把这些习题的解答汇集成册, 并不断增加一些新的问题; 2002 年起又将手写稿不断完善成打印稿, 当时都是为自己教学上的方便(有些难题同学问到, 我们有时也难以当场作答), 从未打算正式出版。近年来, 不少同学和青年教师口头或来信索要这份材料。经过反复和认真考虑, 我们决定对原稿进行增删加修订, 并交付出版。

近世代数研究一般的代数结构, 它是大学生代数训练的一门重要课程。这种训练不仅对于数学系学生是很基本的, 而且由于数字计算和数字通信的发展, 近世代数目前已成为通信和计算机科学的重要数学工具。目前我国高等学校近世代数的教学有很大改进和完善的余地。在代数研究方面有一定实力或教师梯队较强的高校, 代数教学具有好的水准, 学生受到较为充分的近世代数训练。而另有部分学校的近世代数为选修课, 学时少并且没有后续课程, 不少学生只是听到一些莫名其妙的定义和定理, 做一点形式逻辑的推导, 没有领会到这门课程的真谛; 并且在考试之后, 就把学到的一点知识几乎忘光了。

对于二年级或三年级大学生来说, 学习近世代数这门课普遍感到比较抽象, 但是抽象恰恰是数学的基本特性之一, 也是数学训练的一个重要方面。在这门课程中应当让学生学会抽象的思维方式, 如何从许多具体的数学研究对象中提炼出它们的本质 (群、环、域的定义), 并且从这些本质的共性中推导出其他共性 (各种类型群、环、域的公共性质), 如何对研究对象进行合理的分类, 学会不同研究对象之间的比较方式 (即同态), 并以此来研究各种对象的代数结构。这些数学思考方式的训练不仅对整个数学领域是重要的, 而且对于其他科学领域 (乃至于社会生活) 也是基本的。

要使学生受到这种训练, 首先需要大量的例子。在学习近世代数的时候, 学生所熟悉的例子主要来自初等数论和高等代数。一般来说, 高等代数的教学效果还可以, 这门课提供向量空间和多项式环的例子, 并且初步学习了抽象思考方式: 向量空间之间的同态 (线性映射), 子空间和商空间, 二次型的分类, 实或复系数多项式的零点, 带余除法和因子分解 (这本质上是在讲 $\mathbb{C}[x]$ 和 $\mathbb{R}[x]$ 是主理想整环)。同时又使学生感受到这些抽象思考方式和方法是有用的: 它给出线性方程组的完整解法, 给出欧式空间中二次曲面的完整分类, 也给出解一元高次方程的初步手段。另一方面, 初等数论中的模 m 同余类环和它的可逆元构成的集合给

出有限交换群的例子, 还是近世代数许多概念的源头 (元的阶, 循环群和它的生成元, 环的直和 – 中国剩余定理等等)。由于多数学生事先没有初等数论的 “代数化” 训练, 教师在课时本来就不多的近世代数课上先补授初等数论的相关内容, 也很难使学生吃透。这本习题集的目的之一是给学生和教师提供更多的例子。除了原教材中的习题之外, 这次出版前增加了不少我们认为有意义的新例子; 每节前也加上了 “知识要点”。由于有限域在理论和应用上的重要性以及它在学习过程中的有趣性, 我们增加了 “有限域上的不可约多项式” 和 “有限域上的线性代数” 两节。对由定义可直接得出结论的, 只指出此点而未详述。

我们还需要解决学习动机的问题: 为什么需要学这门课程? 善于思考的同学甚至会问: 为什么非要研究群、环和域, 而不研究其他的代数结构? 在这个课程中, 我们无法讲授群、环、域在物理和通信等方面的广泛应用, 但是可以展示几何对称的群论意义, 集合在群作用下的分类和计数。我们还可以做的, 是讲述群的起源和它在数学发展中的作用, 即域的 Galois 理论和用它来解决几个古代数学问题。这会使一部分学生欣赏到数学的优美, 并且从历史中真切地认识到, 除了应用的动力, 数学本身的追求真谛和完美也是重要和不可缺少的。可惜由于学时所限, 上述精品内容在课上无法讲授。我们在习题中作了补充, 例如对 Galois 理论基本定理和代数方程根式可解性定理以习题的形式给出了证明; 对于 “同构延拓定理”, 也以习题的形式给出了它的强形式。

总之, 这本习题集的出版, 目的是帮助同学和年轻教师进一步了解近世代数的真谛, 掌握它的思想和方法, 提高抽象思维能力。对于只想走捷径、应付作业和考试的同学, 它似乎没有太大的益处, 因为要真正读懂这些习题的解答也需要认真思考。一个习题的解答通过简单的照搬, 很难成为另一个习题的解答。

北京师范大学张英伯教授仔细审阅了全书, 给予热情支持并提出宝贵意见。北京航空航天大学李尚志教授和同济大学查建国教授一直关心此项工作。华东师范大学周青教授给予支持和关心。上海交通大学姜翠波教授和武同锁教授督促我们尽快完稿。2003 年, 当时的中国科学技术大学自动化系研究生胡可、计算机系研究生张大力、数学系本科生张伟、数学系研究生赵青、程智先后主动提出帮助打印本书最初的手写稿。中国科学技术大学叶郁教授和山东大学黄华林教授帮助校对。我们一并致谢!

作者欢迎读者提出宝贵意见。

冯克勤　于清华大学
章　璞　于上海交通大学
2009 年 1 月 10 日

目　　录

第一部分　问题总汇

第二部分 问题解答

第一部分　问题总汇

第 1 章　群　论

§1　集合与映射

1.1.1. 设 B, A_i $(i \in I)$ 均是集合 Ω 的子集, 试证:

(1) $B \bigcap \left(\bigcup\limits_{i \in I} A_i \right) = \bigcup\limits_{i \in I} (B \bigcap A_i)$.

(2) $B \bigcup \left(\bigcap\limits_{i \in I} A_i \right) = \bigcap\limits_{i \in I} (B \bigcup A_i)$.

(3) $\overline{\bigcup\limits_{i \in I} A_i} = \bigcap\limits_{i \in I} \overline{A_i}$.

(4) $\overline{\bigcap\limits_{i \in I} A_i} = \bigcup\limits_{i \in I} \overline{A_i}$.

1.1.2. 设 $f:\ A \longrightarrow B$ 是集合的映射 (A, B 是非空集合), 试证:

(1) f 为单射 $\Longleftrightarrow$ 存在 $g:\ B \longrightarrow A$, 使得 $gf = 1_A$.

(2) f 为满射 $\Longleftrightarrow$ 存在 $h:\ B \longrightarrow A$, 使得 $fh = 1_B$.

1.1.3. 如果 $f:\ A \longrightarrow B$, $g:\ B \longrightarrow C$ 均是一一对应, 则 $gf:\ A \longrightarrow C$ 也是一一对应, 且 $(gf)^{-1} = f^{-1}g^{-1}$.

1.1.4. 设 A 是有限集, $P(A)$ 是 A 的全部子集 (包括空集) 所构成的集族. 试证 $|P(A)| = 2^{|A|}$. 换句话说, n 元集合共有 2^n 个不同的子集.

1.1.5. 设 $f:\ A \longrightarrow B$ 是集合的映射. 在集合 A 上如下定义一个关系: 对任意 a, $a' \in A$, $a \sim a'$ 当且仅当 $f(a) = f(a')$. 试证这样定义的关系是一个等价关系.

1.1.6. 设 A, B 是两个有限集合, 则

(1) A 到 B 的不同映射共有多少个?

(2) A 上不同的二元运算共有多少个?

(3) A 到 B 的单射共有多少个?

1.1.7*. 证明等价关系的三个条件是互相独立的, 即: 已知任意两个条件不能推出第三个条件.

1.1.8*. 设 V 是数域上的线性空间, 证明 V 有一组基.

§2 群 的 概 念

1.2.1. 令 N 是所有 $n \times n$ 上三角非奇异复方阵的集合, P 是主对角线上的元都是 1 的上三角方阵的集合, 运算定义为矩阵的乘法. 试证 N 和 P 都是群.

1.2.2. 令 G 是实数对 (a, b), $a \neq 0$ 的集合, 在 G 上定义 $(a, b)(c, d) = (ac, ad + b)$. 试证 G 是群.

1.2.3. 令 Ω 是任意一个集合, G 是一个群, G^{Ω} 是 Ω 到 G 的所有映射的集合. 对任意两个映射 $f, g \in G^{\Omega}$, 定义乘积 fg 是这样的映射: 对任意 $a \in \Omega$, $(fg)(a) = f(a)\, g(a)$. 试证 G^{Ω} 是群.

1.2.4. 令 G 是所有秩不大于 r 的 $n \times n$ 复方阵的集合, 试证在矩阵的乘法下 G 成半群.

1.2.5. 举出一个半群的例子, 它不是含幺半群; 再举出一个含幺半群的例子, 它不是群.

1.2.6*. (这可作为群的另一定义, 即群的单边定义) 设 G 是一个半群, 如果

(a) G 中含有左幺元 e, 即对任意 $a \in G$, $ea = a$.

(b) G 的每个元 a 有左逆 a^{-1}, 使得 $a^{-1} \cdot a = e$.

试证 G 是群.

1.2.7*. (这可作为群的另一定义: 即群的除法定义) 设 G 是半群, 若对任意 a, $b \in G$, 方程 $xa = b$ 和 $ay = b$ 在 G 内有解, 则 G 是群.

1.2.8*. (这可作为有限群的另一定义) 设 G 是一个有限半群, 如果在 G 内左右消去律均成立, 即由 $ax = ay$ 或 $xa = ya$ 可推出 $x = y$, 则 G 是群.

1.2.9. 设 G 是含幺半群, a, $b \in G$.

(1) 如果 a 有逆元 a^{-1}, 则 a^{-1} 也有逆元且 $(a^{-1})^{-1} = a$.

(2) 如果 a 和 b 都具有逆元, 则 ab 也有逆元, 且 $(ab)^{-1} = b^{-1}a^{-1}$.

1.2.10. 设 $f : G \longrightarrow H$ 是群的同态, 则 $f(1_G) = 1_H$; 且对任意 $x \in G$ 有 $f(x^{-1}) = f(x)^{-1}$.

1.2.11. 对任意 $a \in G$, $a \mapsto a^{-1}$ 是群 G 的自同构当且仅当 G 是 Abel 群.

1.2.12. 证明有理数加法群 $\mathbb{Q}$ 和非零有理数乘法群 $\mathbb{Q}^*$ 不同构.

1.2.13. 证明:

(1) 有理数加法群 $\mathbb{Q}$ 和正有理数乘法群 $\mathbb{Q}^+$ 不同构.

(2) 实数加法群 $\mathbb{R}$ 同构于正实数乘法群 $\mathbb{R}^+$.

1.2.14*. 在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解.

1.2.15*. 令 G 是 n 阶有限群, S 是 G 的一个子集, $|S| > \frac{n}{2}$. 试证对任意 $g \in G$, 存在 $a, b \in S$ 使得 $g = ab$.

1.2.16*. 求有理数加法群 $\mathbb{Q}$ 的自同构群 $\mathrm{Aut}(\mathbb{Q})$.

1.2.17*. b 是含幺半群 G 中的元 a 的逆元当且仅当成立 $aba = a$, $ab^2a = 1$.

1.2.18*. 令 G 是 n 阶有限群, $a_1, a_2, \cdots, a_n$ 是群 G 的任意 n 个元, 不一定两两不同. 试证存在整数 p 和 q, $1 \leqslant p \leqslant q \leqslant n$, 使得 $a_p a_{p+1} \cdots a_q = 1$.

1.2.19*. 群 G 的自同构 α 称为没有不动点的自同构, 是指对 G 的任意元 $g \neq 1$ 有 $\alpha(g) \neq g$. 如果有限群 G 具有一个没有不动点的自同构 α 且 $\alpha^2 = 1$, 则 G 一定是奇数阶 Abel 群.

1.2.20*. 设 a, b 是群 G 的两个元, 满足 $aba = ba^2b, a^3 = 1, b^{2n-1} = 1$. 试证 $b = 1$.

§3　子群和陪集分解

1.3.1. 设 A 是群 G 的非空子集, 试证 A 是 G 的子群当且仅当对任意元 $a, b \in A, ab^{-1} \in A$ (这也相当于 $AA^{-1} = A$).

1.3.2. 设群 G 中元 g 的阶 $o(g) = mn$, $(m, n) = 1$. 则 $g = ab$, $o(a) = m$, $o(b) = n$, 且 a, b 均为 g 的幂.

1.3.3. 设群 G 中两个元 g, h 可换, $o(g) = m$, $o(h) = n$. 记 (m, n), $[m, n]$ 分别是 m, n 的最大公因子和最小公倍数. 则

(1) $o(g^n h^m) = \dfrac{[m, n]}{(m, n)}$;

(2) G 中存在阶为 (m, n) 的元;

(3) G 中存在阶为 $[m,n]$ 的元.

1.3.4. 设 A 是群 G 的有限子集, 则 A 是 G 的子群当且仅当对任意元 a, $b \in A$, $ab \in A$.

1.3.5. 设 A, B 分别是群 G 的两个子群, 试证 $A \bigcup B$ 是 G 的子群当且仅当 $A \leqslant B$ 或 $B \leqslant A$. 利用这个事实证明群 G 不能表示成两个真子群的并.

1.3.6. 设 A, B 是群 G 的两个子群, 试证 $AB \leqslant G$ 当且仅当 $AB = BA$.

1.3.7. 设 A, B 是群 G 的两个子群且 $G = AB$. 如果子群 C 包含 A, 则 $C = A(B \bigcap C)$.

1.3.8. 设 A 和 B 是有限群 G 的两个非空子集. 若 $|A| + |B| > |G|$, 则 $G = AB$.

1.3.9. 设 A 和 B 均为群 G 的子群, 则

(1) $g(A \bigcap B) = gA \bigcap gB$, $\forall\ g \in G$.

(2) 若 A 和 B 均有有限的指数, 则 $A \bigcap B$ 也有有限的指数.

1.3.10. 如果 R 是群 G 对于子群 A 的右陪集代表元系, 则 R^{-1} 是群 G 对于 A 的左陪集代表元系.

1.3.11. 设 $A \leqslant G$, $B \leqslant G$. 如果存在 a, $b \in G$, 使得 $Aa = Bb$, 则 $A = B$.

1.3.12. 设 $n > 2$, 则有限群 G 中有偶数个阶为 n 的元.

1.3.13. 设 a, b 是群 G 的任意两个元, 试证 a 和 a^{-1}, ab 和 ba 有相同的阶.

1.3.14*. 设 $A \leqslant G$, 试证 $C_G C_G C_G(A) = C_G(A)$.

1.3.15*. 试证有限群 G 的一个真子群的全部共轭子群之并不能覆盖整个群 G. 结论对无限群是否成立?

1.3.16*. 设 H 和 K 分别是有限群 G 的两个子群, 试证:

$$|HgK| = |H|[K : K \bigcap g^{-1}Hg] = |K|[H : H \bigcap gKg^{-1}].$$

1.3.17*. 设 A 是群 G 的具有有限指数的子群, 试证: 存在 G 的一组元 g_1, $g_2, \cdots, g_m$, 它们既可以作为 A 在 G 中的右陪集代表元系, 又可以作为 A 在 G

中的左陪集代表元系.

1.3.18*. 令 $G=GL(n,\mathbb{C})$, P 是主对角线上的元均为 1 的 $n\times n$ 上三角方阵全体形成的 G 的子群. 确定 $N_G(P), C_G(P)$ 和 P 的中心 $Z(P)$.

1.3.19*. 设 G 是有限 Abel 群, 试证 g 对应到 g^k 是 G 的一个自同构当且仅当 k 和 $|G|$ 互素.

1.3.20*. 设 G 是奇数阶有限群, $\alpha\in \mathrm{Aut}(G)$ 且 $\alpha^2=1$. 令

$$G_1=\{g\in G\,|\,\alpha(g)=g\},\quad G_{-1}=\{g\in G\,|\,\alpha(g)=g^{-1}\}.$$

试证: $G=G_1G_{-1}$ 且 $G_1\bigcap G_{-1}=1$.

1.3.21*. 设群 G 的元 a_1, a_2, b_1, b_2 满足

$$a_1b_1 = a_2b_2 = b_1a_1 = b_2a_2,\quad a_1^m = a_2^m = b_1^n = b_2^n = 1,$$

其中 m 和 n 是互素的正整数. 则 $a_1=a_2$, $b_1=b_2$.

§4 循 环 群

1.4.1. 证明 Euler 定理: 若 n 是正整数, a 是与 n 互素的整数, 则 $a^{\varphi(n)}\equiv 1 \pmod n$, 其中 $\varphi(n)$ 是 Euler 函数, 即 $\varphi(n)$ 是与 n 互素的不超过 n 的正整数的个数.

特别地, 若 p 是素数, 则得到 Fermat 小定理: $a^p\equiv a \pmod p$, $\forall\, a\in\mathbb{Z}$.

1.4.2. 设 n 是正整数, 试证: 满足方程 $x^n=1$ 的复数的集合 G 在通常乘法下是一个 n 阶循环群.

1.4.3. 群 G 没有非平凡子群的充分必要条件是 $G=\{1\}$ 或是素数阶循环群.

1.4.4. (1) 设 a 和 b 是群 G 的元, 阶数分别是 n 和 m, $(n,m)=1$ 且 $ab=ba$. 求 $|\langle ab\rangle|$.

(2) 设群 G 中元 g 的阶 $o(g)$ 与正整数 n 互素, 在 $\langle g\rangle$ 中求解方程 $x^n=g$.

1.4.5. 真子群 M 称为群 G 的极大子群, 如果不存在 G 的子群 B 使得 $M<B<G$. 确定无限循环群的全部极大子群.

1.4.6*. 如果有限群 G 有唯一的极大子群, 则 G 是素数幂阶循环群.

1.4.7. 举一个无限群的例子, 它的任意阶数不为 1 的子群都具有有限指数.

1.4.8. 设 p 是一个素数, $G = \{x \in \mathbb{C} \mid 存在正整数\ n\ 使得\ x^{p^n} = 1\}$, 则 G 对于复数的乘法作成群. 试证 G 的任意真子群都是有限阶的循环群.

1.4.9. 若群 G 只有有限多个子群, 则 G 是有限群.

1.4.10*. 有理数加法群 $\mathbb{Q}$ 不是循环群, 但它的任意有限生成的子群都是循环群.

1.4.11*. 在 n 阶循环群 G 中, 对 n 的每个正因子 m, 阶为 m 的元恰好有 $\varphi(m)$ 个, 其中 $\varphi(m)$ 是与 m 互素且不超过 m 的正整数的个数. 由此证明等式 $\sum\limits_{m|n} \varphi(m) = n$.

1.4.12*. 设 G 是一个 n 阶有限群, 若对 n 的每一个因子 m, G 中至多只有一个 m 阶子群, 则 G 是循环群.

1.4.13*. 群 G 是循环群当且仅当 G 的任一子群形如 $G^m = \{g^m | \ g \in G\}$, 其中 m 是非负整数.

§5 正规子群和商群

1.5.1. 令 G 是实数对 (a, b), $a \neq 0$ 带有乘法 $(a, b)(c, d) = (ac, ad + b)$ 的群. 试证:$K = \{(1, b) | \ b \in \mathbb{R}\}$ 是 G 的正规子群且 $G/K \cong \mathbb{R}^*$, 这里 $\mathbb{R}^*$ 是非零实数的乘法群.

1.5.2. 设 G 是群, $N < M < G$.

(1) 如果 $N \lhd G$, 则 $N \lhd M$.

(2) 如果 $N \lhd M$, $M \lhd G$, N 是否一定是 G 的正规子群?

1.5.3. 试证:

(1) 群 G 的中心 $Z(G)$ 是 G 的正规子群.

(2) 群 G 的指数为 2 的子群 N 一定是 G 的正规子群.

1.5.4. (1) 设 $N \lhd G$, M 是 G 的子群且 $N \leqslant M$. 则 $N_G(M)/N = N_{\overline{G}}(\overline{M})$, 这里 $\overline{G} = G/N$, $\overline{M} = M/N$.

(2) 设 $f: G \longrightarrow H$ 是群同态, $M \leqslant G$. 试证 $f^{-1}(f(M)) = KM$, 这里 $K = \operatorname{Ker} f$.

(3) 设 $f: G \longrightarrow H$ 是群同态. 若 g 是 G 的一个有限阶元, 则 $f(g)$ 的阶整除 g 的阶.

1.5.5. 设 M 和 N 分别是群 G 的正规子群. 如果 $M \bigcap N = 1$, 则对任意 $a \in M$, $b \in N$ 有 $ab = ba$.

1.5.6. 设 $N \lhd G$, g 是群 G 的任意一个元. 若 g 的阶和 $|G/N|$ 互素, 则 $g \in N$.

1.5.7. 如果 $G/Z(G)$ 是循环群, 则 G 是 Abel 群.

1.5.8*. 用 $I(G)$ 表示 G 的全部内自同构组成的集合. 试证: $I(G) \leqslant \mathrm{Aut}(G)$, 且 $I(G) \cong G/Z(G)$.

1.5.9*. 试证非可换群 G 的自同构群 $\mathrm{Aut}(G)$ 不是循环群.
特别地, 若群 G 只有素数个自同构, 则 G 是可换群.

1.5.10*. 用 $[G,G]$ 表示群 G 的换位子群, 即由所有换位子 $[g,h] = ghg^{-1}h^{-1}$, $g,h \in G$ 生成的 G 的子群; 记 $G^{(1)} = [G,G]$, $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$, $\forall\ n > 1$. 则 $G^{(n)}$ 均是 G 的正规子群, $\forall\ n \geqslant 1$.

1.5.11. 设 $N \lhd G$, $N \bigcap [G,G] = \{1\}$, 则 $N \leqslant Z(G)$.

1.5.12*. 群 G 的非平凡子群 N 称为 G 的极小子群, 如果不存在子群 B 使得 $1 \subsetneqq B \subsetneqq N$. 试证:
(1) 整数加法群 $\mathbb{Z}$ 没有极小子群.
(2) 有理数加法群 $\mathbb{Q}$ 既没有极小子群也没有极大子群.

1.5.13*. 设 α 是有限群 G 的自同构. 令 $I = \{g \in G \mid \alpha(g) = g^{-1}\}$. 试证:
(1) 若 $|I| > \dfrac{3}{4}|G|$, 则 G 是 Abel 群.
(2) 若 $|I| = \dfrac{3}{4}|G|$, 则 G 一定有指数为 2 的 Abel 正规子群.

§6 置 换 群

1.6.1. 把置换 $\sigma = (4\,5\,6)(5\,6\,7)(7\,6\,1)$ 写成不相交轮换的积.

1.6.2. 讨论置换

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$$

的奇偶性.

1.6.3. 一个置换的阶等于它的轮换表示中各个轮换因子的长度的最小公倍数.

1.6.4. 设 $\sigma=(1\,2\cdots n)\in S_n$, 证明: $C_{S_n}(\sigma)=\langle\sigma\rangle$.

1.6.5. 试证当 $n\geqslant 3$ 时, 中心 $Z(S_n)=\{1\}$.

1.6.6. 当 $n\geqslant 3$ 时, 试证 $n-2$ 个 3 轮换 $(1\,2\,3)$, $(1\,2\,4)$, $\cdots$, $(1\,2\,n)$ 是 A_n 的生成元.

1.6.7. 试证 A_4 没有 6 阶子群.

1.6.8. 设 σ_1 和 σ_2 是 S_n 中的两个偶置换. 若 σ_1 和 σ_2 在 S_n 中共轭, 则它们在 A_n 中也一定共轭吗?

1.6.9*. 确定 S_4 的全部正规子群.

1.6.10*. 试证:

(1) 对称群 S_n 是交错群 A_{2n} 的子群.

(2) 每个有限群均是某个交错群的子群.

1.6.11*. S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $n!/\prod\limits_{i=1}^{n}i^{\lambda_i}\lambda_i!$ 个, 由此证明

$$\sum_{\lambda}\frac{1}{\prod\limits_{i=1}^{n}i^{\lambda_i}\lambda_i!}=1,$$

其中 λ 取遍所有的型, 即 λ 取遍所有的数组 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$, λ_i 均为非负整数且满足 $\lambda_1+2\lambda_2+\cdots+n\lambda_n=n$.

1.6.12*. 当 $n\geqslant 2$ 时, 试证 $(1\,2)$ 和 $(1\,2\,3\cdots n)$ 是 S_n 的一组生成元.

§7 群在集合上的作用

1.7.1. 设 G 作用在集合 S 上, 对任意 $a,b\in S$, 若存在 $g\in G$ 使得 $ga=b$, 则 $G_a=g^{-1}G_bg$. 换句话说, 同一轨道中元的固定子群彼此共轭.

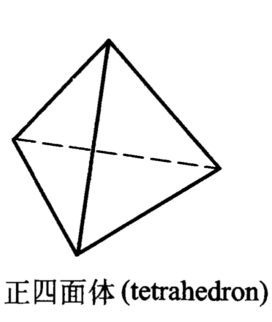
1.7.2. 设群 G 在集合 S 上的作用是可迁的, N 是 G 的正规子群, 则 S 在 N 作用下的每个轨道有同样多的元.

1.7.3*. (Burnside 引理) 设群 G 作用在集合 S 上, 令 t 表示 S 在 G 作用下的轨道的条数. 对任意 $g \in G$, $F(g)$ 表示 S 在 g 作用下不动点的个数, 即 $F(g) = |\{x \in S | gx = x\}|$. 试证

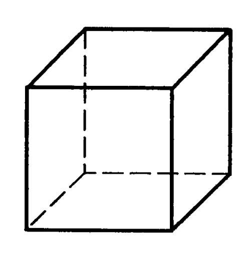
$$t = \frac{\sum\limits_{g \in G} F(g)}{|G|}$$

这就是说, G 的每个元在 S 上作用平均使得 t 个文字不动.

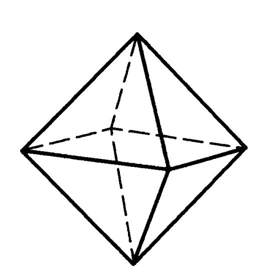
1.7.4. 求正四面体、正六面体、正八面体、正十二面体和正二十面体 (如下图所示) 的旋转群和对称群各有多少个元?



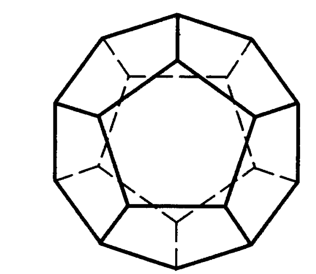
正四面体 (tetrahedron)

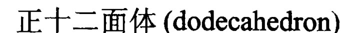


正六面体(hexahedron)

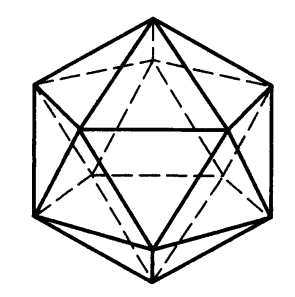


正八面体 (octahedron)





正十二面体 (dodecahedron)



正二十面体 (icosahedron)

1.7.5*. 设 p 是一个素数, G 是 p 的方幂阶的群. 试证 G 的非正规子群的个数一定是 p 的倍数.

1.7.6*. 令 G 是一个单群, 如果存在 G 的真子群 H 使得 $[G:H] \leqslant 4$, 则 $|G| \leqslant 3$.

1.7.7*. 设 H 是群 G 的指数为 $n < \infty$ 的真子群, 试证 H 一定含有 G 的一个有有限指数的真正规子群.

如果还有 $|G| > n!$, 则 G 不是单群.

1.7.8*. 试证一般线性群 $GL(n, \mathbb{C})$ 不含有指数有限的真子群.

1.7.9*. 求对称群 S_3 的自同构群 $\mathrm{Aut}(S_3)$.

1.7.10*. 令 G 是阶数为 $2^n m$ 的群, 其中 m 是奇数. 如果 G 含有一个 2^n 阶的元, 则 G 含有一个指数为 2^n 的正规子群.

1.7.11*. 设 α 是有限群 G 的一个自同构. 若 α 把每个元都变到它在 G 中的共轭元, 即对任意 $g \in G$, g 和 $\alpha(g)$ 共轭, 则 α 的阶的每个素因子都是 $|G|$ 的因子.

1.7.12*. 设 p 是 $|G|$ 的最小素因子. 若 p 阶子群 $A \lhd G$, 则 $A \leqslant Z(G)$.
特别地, p- 群 G 的 p 阶正规子群含于 G 的中心.

§8 Sylow 定理

1.8.1. 设 p 是 $|G|$ 的素因子, 则 G 有 p 阶元.

1.8.2. 设 p 是 $|G|$ 的素因子, 则方程 $x^p = 1$ 在 G 中的解的个数是 p 的倍数.

1.8.3. 证明 6 阶非 Abel 群只有 S_3.

1.8.4. 200 阶群有正规的 Sylow 子群.

1.8.5. 确定 S_4 的 Sylow 子群的个数.

1.8.6. 设 P 是有限群 G 的 Sylow p- 子群, $N_G(P) \lhd G$. 证明 $P \lhd G$.

1.8.7. 设 N 是有限群 G 的正规子群. 若素数 p 和 $|G/N|$ 互素, 则 N 包含 G 的所有 Sylow p- 子群.

1.8.8. 设 N 是有限群 G 的正规子群, P 是 G 的 Sylow p- 子群. 则
(1) $N \bigcap P$ 是 N 的 Sylow p- 子群.
(2) PN/N 是 G/N 的 Sylow p- 子群.
(3) $(N_G(P)N)/N = N_{G/N}(PN/N)$.

1.8.9. 设 G 是集合 Σ 上的置换群, P 是 G 的 Sylow p- 子群, $a \in \Sigma$. 若 $p^m \mid |Ga|$, 则 $p^m \mid |Pa|$.

1.8.10. 确定恰有 3 个共轭类的有限非交换群 G.

1.8.11. 设 P 是有限群 G 的 Sylow p- 子群, H 是 G 的子群, $P| \; |H|$. 则存在 $a \in G$ 使得 $aPa^{-1} \bigcap H$ 是 H 的 Sylow p- 子群.

1.8.12. 24, 36, 48 阶群均非单.

1.8.13*. 确定 S_4 的自同构群 $\mathrm{Aut}(S_4)$.

1.8.14*. 设 $P_1, \cdots, P_t$ 是有限群 G 的全部 Sylow p- 子群. 若对 $i \neq j, 1 \leqslant i \leqslant t, 1 \leqslant j \leqslant t$, 总有 $[P_i : P_i \bigcap P_j] \geqslant p^r$, 则 $t \equiv 1 (\mathrm{mod}\ p^r)$.

1.8.15*. 设 G 是集合 Σ 上的置换群, $a \in \Sigma$, P 是固定子群 G_a 的 Sylow p-子群, $\triangle$ 是轨道 Ga 在 P 作用下的全部不动点的集合. 证明 $N_G(P)$ 在 $\triangle$ 上的作用是可迁的.

1.8.16*. 设 G 是 24 阶群且中心 $Z(G) = 1$, 证明 $G \cong S_4$.

§9 自由群和群的表现

1.9.1. 设 G_i $(1 \leqslant i \leqslant n)$ 为群, $N_i \leqslant G_i$, 则

(1) $G_1 \times G_2 \cong G_2 \times G_1$.

(2) $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$.

(3) $Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n)$.

(4) $G_1 \times \cdots \times G_n$ 为 Abel 群当且仅当每个 G_i 均为 Abel 群.

(5) $N_1 \times \cdots \times N_n \leqslant G_1 \times \cdots \times G_n$.

(6) $N_1 \times \cdots \times N_n \lhd G_1 \times \cdots \times G_n$ 当且仅当对每个 i, $N_i \lhd G_i$.

(7) 当 $N_1 \times \cdots \times N_n \lhd G_1 \times \cdots \times G_n$ 时, $(G_1 \times \cdots \times G_n)/(N_1 \times \cdots \times N_n) \cong (G_1/N_1) \times \cdots \times (G_n/N_n)$.

1.9.2. 若 $n \geqslant 3$, 试问 $A_n \times \mathbb{Z}_2$ 与 S_n 是否同构?

1.9.3. 设 $G = G_1 \times \cdots \times G_n$, H 是 G 的子群. 问 H 是否一定形如 $H = H_1 \times \cdots \times H_n$, 其中 $H_i \leqslant G_i$?

1.9.4. 设 $G = G_1 \times G_2$, $H \lhd G$ 且 $H \bigcap G_i = \{1\}$, $i = 1, 2$. 试证 $H \leqslant Z(G)$. 特别地, H 是 Abel 群.

1.9.5. 令 $G = G_1 \times \cdots \times G_n$, 且对任意 $i \neq j$, $|G_i|$ 和 $|G_j|$ 互素. 则 G 的任意子群 H 都是它的子群 $H \bigcap G_i$ $(i = 1, \cdots, n)$ 的直积.

1.9.6. 设 G 是有限生成的自由 Abel 群, $\mathrm{rank}(G) = r$. 如果 $g_1, \cdots, g_n$ 是 G 的一组生成元, 则 $n \geqslant r$.

1.9.7. 如果 n 是正奇数, 求证 $D_{2n} \cong D_n \times Z_2$.

1.9.8. 以 $\mathbb{C}^*$ 表示非零复数乘法群, $\mathbb{R}^+$ 为正实数乘法群, $\mathbb{R}$ 为实数加法群, $\mathbb{Z}$ 为整数加法群, 则 $\mathbb{C}^* \cong \mathbb{R}^+ \times \mathbb{R}/(2\pi\mathbb{Z})$.

1.9.9. 设 $n_1, \cdots, n_r$ 为自然数, 则

(1) $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cong Z_{n_1 n_2}$ 当且仅当 $(n_1, n_2) = 1$.

(2) 如果 $n_1, \cdots, n_r$ 两两互素, 则 $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \cong \mathbb{Z}_{n_1 \cdots n_2}$.

1.9.10. 试证 $7 \cdot 11 \cdot 13$ 阶群一定是循环群.

1.9.11*. 试证 $5 \cdot 7 \cdot 13$ 阶群为循环群.

1.9.12*. 设 G_1 和 G_2 是两个非交换单群, 试证 $G_1 \times G_2$ 的非平凡正规子群只有 G_1 和 G_2.

1.9.13*. 令 $G = \langle g_1,\ g_2, \cdots,\ g_n \rangle$. 如果 G 的子群 A 具有有限指数 m, 则 A 可以由 $2nm$ 个元生成.

1.9.14*. 试证: 定义关系为

$$x_i^2 = 1,\ i = 1, \cdots, n-1,$$

$$x_i x_j = x_j x_i,\quad i \text{ 与 } j \text{ 不相邻 (即 } j < i-1),$$

$$(x_i x_{i+1})^3 = 1,\ i < n-2 \quad (\text{即}\quad x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1})$$

的 $n-1$ 个元 $x_1, \cdots, x_{n-1}$ 生成的群 G_n 同构于对称群 S_n.

1.9.15*. 试证: 对 $n \geqslant 3$, 定义关系为

$$x_1^3 = 1,$$

$$x_i^2 = 1,\ i = 2, \cdots, n-2,$$

$$(x_i x_{i+1})^3 = 1,\ i = 1, \cdots, n-3,$$

$$(x_i x_j)^2 = 1,\ i = 1, \cdots, n-4,\ j > i+1$$

的 $n-2$ 个元 $x_1, \cdots, x_{n-2}$ 生成的群 G_n 同构于交错群 A_n.

§10 有限生成 Abel 群

1.10.1. 用不变因子的方式写出所有互不同构的 360 阶 Abel 群.

1.10.2. 试证: 有限生成 Abel 群 G 是有限群当且仅当 G 的一组生成元均是有限阶元.

1.10.3*. 试证有限生成 Abel 群 G 是自由 Abel 群当且仅当 G 的每个非零元都是无限阶元.

1.10.4*. 设 $\mathbb{Q}^+$ 是正有理数乘法群, 试证:

(1) $\mathbb{Q}^+$ 是自由 Abel 群, $\{p \mid p$ 是素数$\}$ 是它的一组基.

(2) $\mathbb{Q}^+$ 不是有限生成的.

1.10.5*. 设 $\mathbb{Q}$ 是有理数加法群, 试证:

(1) $\mathbb{Q}$ 不是自由 Abel 群.

(2) $\mathbb{Q}$ 的任意有限生成的子群都是循环群, 但 $\mathbb{Q}$ 不是循环群.

1.10.6. 设 A 为有限 Abel 群, 则对于 $|A|$ 的每个正因子 d, A 均有 d 阶子群和 d 阶商群.

1.10.7. 设 H 是有限 Abel 群 A 的子群, 则有 A 的子群同构于 A/H.

1.10.8. 如果有限 Abel 群 A 不是循环群, 则存在素数 p 使得 A 有子群同构于 $\mathbb{Z}_p^2 = \mathbb{Z}_p \oplus \mathbb{Z}_p$.

1.10.9. 试证: 当 $(m, n) = 1$ 时, $\mathbb{Z}_m \oplus \mathbb{Z}_n$ 的不变因子组为 $\{mn\}$; 而当 $(m, n) > 1$ 时, $\mathbb{Z}_m \oplus \mathbb{Z}_n$ 的不变因子组为 $\{(m, n), [m, n]\}$.

1.10.10. 求 $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{35}$ 的初等因子组和不变因子组.

1.10.11. 试证非零复数乘法群 $\mathbb{C}^*$ 的每个有限子群都是循环群.

1.10.12. 设 G, A, B 均为有限 Abel 群. 如果 $G \oplus A \cong G \oplus B$, 求证 $A \cong B$.

1.10.13*. 设 p 是一个素数, $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ 有多少个 p^2 阶子群?

1.10.14*. 设 G 是 n 个 p 阶群的直和, 问 G 有多少个极大子群?

1.10.15*. 如果有限群 G 的每个极大子群都是单群且都在 G 中正规, 则 G 只能是 p 阶群, 或 p^2 阶群, 或 pq 阶循环群, p, q 是不同的素数.

1.10.16*. 设 $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$, p 是素数, 则 G 有 p 阶自同构.

1.10.17*. 设 $|G| = p^a q^b$, p, q 是不同的素数. 若群 G 没有 p 阶自同构, 则 $a = 0$ 或 1.

§11 小阶群的结构

1.11.1. 求 D_4 和 Q_8 的中心 $Z(D_4)$ 和 $Z(Q_8)$.

1.11.2. 每一子群都是正规子群的群称为 Hamilton 群. 试证 Q_8 是 (非交换的) Hamilton 群.

1.11.3. 设 $|G| = p^n$, $n \geqslant 1$, 则阶为 p^{n-1} 的子群 H 一定是正规的.

1.11.4*. 确定所有互不同构的 18 阶群.

1.11.5*. 确定所有互不同构的 20 阶群.

1.11.6*. 设 p, q 是两个素数, $p < q$. 试证: pq 阶非 Abel 群 G 一定可以由下述生成元和定义关系给出:

$$G = \langle a, b \mid a^p = 1 = b^q, a^{-1}ba = b^r \rangle,$$

其中 $r^p \equiv 1 (\mathrm{mod}\ q)$, q 不整除 $r-1$, p 整除 $q-1$.

1.11.7*. 设 p 是奇素数, 试证 p^3 阶非 Abel 群 G 可以由下述生成元和定义关系给出:

(1) $G = \langle a, b \mid a^{p^2} = b^p = 1,\ b^{-1}ab = a^{1+p} \rangle$.

(2) $G = \langle a, b, c \mid a^p = b^p = c^p = 1,\ ac = ca,\ cb = bc,\ ab = bac \rangle$.

§12 可解群和幂零群

1.12.1. 设 $I^{(1)}(G)$ 是 G 的内自同构群, $I^{(n)}(G)$ 是 $I^{(n-1)}(G)$ 的内自同构群. 试证: G 是幂零群当且仅当存在 $n \geqslant 1$ 使得 $I^{(n)}(G) = \{1\}$.

1.12.2. 设 a 和 b 是有限幂零群 G 的两个元, $a^m = b^n = 1$ 且 $(m, n) = 1$. 试证 $ab = ba$.

1.12.3. 设 G 是有限幂零群, 试证:

(1) 如果 $\{1\} \neq N \lhd G$, 则 $N \bigcap Z(G) \neq \{1\}$.

(2) 设 G 是非 Abel 群, A 是 G 的正规子群集合中的极大元, 且 A 是 Abel 群, 则 $C_G(A) = A$.

1.12.4. 设 a, b 是群 G 的任意两个元. 如果 a, b 和它们的换位子 $[a, b]$ 可交换, 则对任意整数 m 和 n, $[a^m, b^n] = [a, b]^{mn}$.

1.12.5. 设 A, B 是群 G 的两个子群, $[A,B]$ 表示由 $\{[a,b] \mid a \in A, b \in B\}$ 生成的群, $\langle A,B\rangle$ 表示由 $A \bigcup B$ 生成的群. 试证:

(1) $[A,B] \lhd \langle A,B\rangle$.

(2) $A \lhd G$ 当且仅当 $[A,G] \leqslant A$.

(3) 如果 $B \lhd G$ 且 $B \leqslant A$, 则 $A/B \leqslant Z(G/B)$ 当且仅当 $[A,G] \leqslant B$.

1.12.6. 对任意群 G, 定义 $r_1(G) = G$, $r_2(G) = [G,G]$, 一般地, $r_n(G) = [r_{n-1}(G), G]$. 试证: G 是幂零群当且仅当存在 $n \geqslant 1$ 使得 $r_n(G) = \{1\}$.

1.12.7. 求二面体群 D_n 的换位子群, 这里 $D_n = \langle a, b \mid a^n = b^2 = 1, b^{-1}ab = a^{-1}\rangle$.

1.12.8. 试证: 对称群 S_3 和 S_4 是可解群, 但不是幂零群.

1.12.9. 设 $N \lhd G$. 如果 N 和 G/N 均为幂零群, G 是否为幂零群?

1.12.10. 设 $N \leqslant Z(G)$, 试证: 如果 G/N 为幂零群, 则 G 为幂零群.

1.12.11. 设 $G = S_4$, 试证 $G/G^{(2)} \cong S_3$.

1.12.12. 设 A 是群 G 的循环的正规子群. 试证 A 和 G' 按元可交换, 即对任意 $a \in A$, $x \in G'$, $ax = xa$.

1.12.13. 设 α 是群 G 的一个自同构. 如果对任意 $g \in G$, $g^{-1}\alpha(g) \in Z(G)$, 则对导群 G' 的任意元 a, $\alpha(a) = a$.

1.12.14. 设 p, q, r 是三个素数, 不一定不相同, 试证: pqr 阶群是可解群.

1.12.15. 有限群 G 是可解群当且仅当 G 的合成因子均是素数阶循环群.

1.12.16. (1) 求 S_4 的导出列、合成列和合成因子.

(2) 求四元数群 Q_8 的所有合成列.

1.12.17. 设 G 是 p^3 阶非交换群, p 为素数. 则 $Z(G) = G^{(1)}$.

1.12.18. 求对称群 S_n 和交替群 A_n 的导出列.

1.12.19. 阶为素数幂的群 G 是可解群.

1.12.20. 对于有限群 G 来说, 下述命题等价:

(1) G 是可解群, 即有正整数 n 使得 $G^{(n)} = \{1\}$, 其中 $G^{(n)}$ 是 G 的第 n 次导群.

(2) G 有终止于 $\{1\}$ 的正规群列, 即存在 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\}$, 且 $G_i \lhd G$, $1 \leqslant i \leqslant m$, 使得每个因子群 G_{i-1}/G_i 均为 Abel 群, $1 \leqslant i \leqslant m$.

(3) G 有终止于 $\{1\}$ 的次正规群列, 即存在 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\}$, 使得每个因子群 G_{i-1}/G_i 均为 Abel 群, $1 \leqslant i \leqslant m$.

(4) G 有终止于 $\{1\}$ 的次正规群列, 使得每个因子群均为素数阶循环群.

(5) G 有终止于 $\{1\}$ 的次正规群列, 使得每个因子群的阶均为素数幂.

第 2 章　环　　论

§1　基 本 概 念

2.1.1.　设 A 是 Abel 群, $\mathrm{End}(A)$ 是群 A 的全部自同态作成的集合. 对 f, $g\in\mathrm{End}(A)$ 定义

$$(f+g)(a)=f(a)+g(a),\quad (f\cdot g)(a)=f(g(a)),\quad \forall\ a\in A.$$

则 $\mathrm{End}(A)$ 对于上述运算是含幺环.

2.1.2. (1)*　举例表明含幺环中, 一个左可逆元可以具有多于一个左逆.

(2)　如果 a 是含幺环中左可逆元, 并且 a 不是右零因子, 则 a 只有唯一的左逆.

2.1.3.　设 a 是环 R 中非零元, 求证:

(1)　a 不是 R 中左零因子当且仅当由等式 $ab=ac$, 其中 $b,c\in R$ 可推出 $b=c$.

(2)　a 不是 R 中右零因子当且仅当由等式 $ba=ca$, 其中 $b,c\in R$ 可推出 $b=c$.

2.1.4.　设 $n\geqslant 2$ 为正整数, 求证:

(1)　环 $\mathbb{Z}_n$ 中元 $\overline{a}$ 可逆当且仅当 $(a,n)=1$.

(2)　若 p 为素数, 则 $\mathbb{Z}_p$ 是域, 若 n 不是素数, 则 $\mathbb{Z}_n$ 不是整环.

2.1.5.　(1) 决定环 $\mathbb{Z}[\sqrt{-1}\,]$ 的单位群, 证明此环为整环但不是域.

(2)　对于环 $\mathbb{Z}[\sqrt{-3}\,]=\{a+b\sqrt{-3}\mid a,b\in\mathbb{Z}\}$ 做同样事情.

2.1.6.　设 R 和 S 均为含幺环, $f:R\longrightarrow S$ 为环的满同态. 则

(1)　$f(1_R)=1_S$.

(2)　设 $0_S\neq 1_S$, 如果 $a\in U(R)$, 则 $f(a)\in U(S)$, 并且 $f(a^{-1})=f(a)^{-1}$.

2.1.7.　设 G 是乘法群, R 为环. 定义集合 $R[G]=\left\{\sum\limits_{g\in G}r_g g\mid r_g\in R\right.$, 并且只有有限多个 $\left.r_g\neq 0\right\}$. 规定 $R[G]$ 中两个元 $\sum\limits_{g\in G}r_g g$ 和 $\sum\limits_{g\in G}t_g g$ 相等当且仅当

$r_g = t_g, \ \forall\, g \in G$. 在集合 $R[G]$ 上定义

$$\sum_{g\in G} r_g g + \sum_{g\in G} t_g g = \sum_{g\in G}(r_g + t_g)g,$$
$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} t_g g\right) = \sum_{g\in G}\left(\sum_{g'g''=g} r_{g'}t_{g''}\right)g.$$

(1) $R[G]$ 对于上述加法和乘法作成环 (叫做群 G 在环 R 上的群环).

(2) $R[G]$ 是交换环当且仅当 R 是交换环且 G 是 Abel 群.

(3) 若环 R 有单位元 1_R, 而群 G 的单位元为 e, 则 $1_R e$ 是群环 $R[G]$ 的幺元.

(4) R 可以自然地看成是 $R[G]$ 的子环.

(5) 设 G 是有限群, R 是交换环. 求群环 $R[G]$ 的中心 $Z(R[G])$.

(6) $R[G]$ 是否为无零因子环?

2.1.8. (1) 整数环 $\mathbb{Z}$ 的加法群自同构是否一定为环的自同构?

(2) 求 $\mathbb{Z}_m$ 的全部子环和 $\mathrm{Aut}(\mathbb{Z}_m)$, 其中 m 为正整数.

2.1.9. (1) 求 $\mathbb{Q}$ 的全部子域.

(2) 求证 $\mathbb{Q}[\sqrt{2}\,] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 是实数域 $\mathbb{R}$ 的子域; 并求 $\mathbb{Q}[\sqrt{2}\,]$ 的全部子域.

(3) 求 $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}\,])$.

2.1.10*. (1) 设 $f \in \mathrm{Aut}(\mathbb{R})$, α, $\beta \in \mathbb{R}$. 若 $\alpha > 0$, 则 $f(\alpha) > 0$. 从而, 若 $\alpha > \beta$, 则 $f(\alpha) > f(\beta)$.

(2) 求 $\mathrm{Aut}(\mathbb{R})$.

2.1.11. (1) 可将复数域 $\mathbb{C}$ 嵌到环 $M_2(\mathbb{R})$ 中吗?

(2) 令 $L = \left\{\begin{pmatrix} z & w \\ -\overline{w} & \overline{z}\end{pmatrix} \middle|\, z, w \in \mathbb{C}\right\}$, 其中 $\overline{w}$ 为 w 的共轭复数, 求证 L 是体, 并且同构于实四元数体 $\mathbb{H}$.

2.1.12. 设 R 为环, 如果每个元 $a \in R$ 均满足 $a^2 = a$, 则称 R 为布尔 (Boole) 环. 求证:

(1) 布尔环 R 必为交换环, 并且 $a + a = 0_R$, $\forall\, a \in R$.

(2) 设 U 是一个集合, S 是 U 的全部子集构成的集族, 即 $S = \{V \mid V \subseteq U\}$.

对于 $A, B \in S$, 定义

$$A - B = \{c \in U \mid c \in A,\ c \notin B\},$$
$$A + B = (A - B)\bigcup(B - A),$$
$$A \cdot B = A\bigcap B.$$

求证 $(S, +, \cdot)$ 是布尔环. 环 S 是否有幺元?

2.1.13*. 试证:

(1) 有限整环必为域.

(2) 只有有限个理想的整环 R 是域.

2.1.14. 以 $C(\mathbb{R})$ 表示全部连续实函数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ 组成的集合. 定义 $(f + g)(a) = f(a) + g(a)$, $(f \cdot g)(a) = f(a) \cdot g(a)$, 对于 $f, g \in C(\mathbb{R})$, $a \in \mathbb{R}$. 求证 $C(\mathbb{R})$ 由此成为含幺交换环. 试问 $C(\mathbb{R})$ 是否为整环? 是否有幂零元? 决定环 $C(\mathbb{R})$ 的单位群.

2.1.15. 设 D 为有限体, 求证 $a^{|D|} = a, \quad \forall\, a \in D$.

2.1.16. 设 G 为二元群, 试决定群环 $\mathbb{Z}[G]$ 的单位群.

2.1.17*. 设 a, b 是含幺环 R 中的元, 则 $1 - ab$ 可逆 $\Longleftrightarrow$ $1 - ba$ 可逆.

2.1.18*. (华罗庚) 设含幺环 R 中元 a, b, $1 - ab$ 均为单位, 则 $a - b^{-1}$ 和 $(a - b^{-1})^{-1} - a^{-1}$ 也是单位, 且

$$((a - b^{-1})^{-1} - a^{-1})^{-1} = aba - a.$$

2.1.19*. (Kaplansky) 含幺环中某元若有多于一个右逆, 则它必然有无限多个右逆.

2.1.20*. (1) (华罗庚, 1949) 设 L 是非可换体, a 是 L 中非中心的元, 则 L 由 a 的所有共轭元生成.

(2) (H. Cartan - R. Brauer - 华罗庚) 设 L 是体, K 是其真子体, 且 $K^* = K - \{0\}$ 是 L^* 的正规子群, 则 K 含于 L 的中心.

§2 环的同构定理

2.2.1. 环 R 中的元 a 叫做幂零的, 是指存在正整数 m 使得 $a^m = 0$.

(1) 若 R 为交换环, a 和 b 均为幂零元, 则 $a + b$ 也是幂零元.

(2) 若 R 不为交换环, (1) 中结论是否仍成立?

(3) 交换环 R 中幂零元的集合 N 是 R 的理想, 且商环 R/N 中只有 0 是幂零元.

2.2.2. 设 I 是交换环 R 中的理想, 求证集合 $\sqrt{I} = \{r \in R \mid 存在\ n \geqslant 1\ 使得\ r^n \in I\}$ 也是环 R 的理想.

2.2.3. 设 R 为环, 集合 $Z(R) = \{c \in R \mid 对于每个\ r \in R, rc = cr\}$ 叫做环 R 的中心.

(1) 求证 $Z(R)$ 是 R 的子环, 但不一定是 R 的理想.

(2) 如果 F 为域, 求证全矩阵环 $M_n(F)$ 的中心为 $\{aI_n \mid a \in F\}$, 其中 I_n 表示 n 阶单位方阵.

2.2.4. (1)* 设 R 为含幺交换环, 求证环 $M_n(R)$ 中每个理想均为形式 $M_n(I)$, 其中 I 是 R 的某个理想.

(2) 若 F 为域, 则 $M_n(F)$ 是单环.

(3) 设 I 是含幺交换环 R 中的理想, 求证有环同构: $M_n(R)/M_n(I) \cong M_n(R/I)$.

2.2.5. 设 I_1 和 I_2 均是环 R 的理想, 求证:

(1) I_1I_2 也是环 R 的理想, 并且 $I_1I_2 \subseteq I_1 \bigcap I_2$. 是否一定有 $I_1I_2 = I_1 \bigcap I_2$?

(2) $I_1 + I_2$ 也是环 R 的理想, 并且它恰好是包含 I_1 和 I_2 的最小理想.

(3) 设 $I_1 = n\mathbb{Z}$, $I_2 = m\mathbb{Z}$ $(n, m \geqslant 1)$ 是整数环 $\mathbb{Z}$ 的两个理想, 求证: $I_1I_2 = nm\mathbb{Z}$, $I_1 + I_2 = (n, m)\mathbb{Z}$, $I_1 \bigcap I_2 = [n, m]\mathbb{Z}$.

2.2.6. 设 $f : R \longrightarrow S$ 是环的同态, I 和 J 分别是环 R 和 S 的理想, 并且 $f(I) \subseteq J$. 按以下方式作商环之间的映射:

$$\overline{f} : R/I \longrightarrow S/J \quad , \quad \overline{a} \mapsto [f(a)],$$

其中, 对于 $a \in R$, $\overline{a} = a + I$ 为 R/I 中的元, 而 $[f(a)] = f(a) + J$ 为 S/J 中的元.

(1) 说明 $\overline{f}$ 是定义合理的, 且是环同态.

(2) $\overline{f} : R/I \longrightarrow S/J$ 是环同构 $\Longleftrightarrow$ $f(R) + J = S$ 并且 $I = f^{-1}(J)$.

2.2.7. 设 $f : R \longrightarrow S$ 是环的同态. 如果 R 是体, 求证 f 或者是零同态, 或者是嵌入.

2.2.8. 设 $(R, +, \cdot)$ 是含幺环. 对于 $a, b \in R$, 定义 $a \oplus b = a + b + 1$, $a \odot b = ab + a + b$. 求证 $(R, \oplus, \odot)$ 也是含幺环, 并且与环 $(R, +, \cdot)$ 同构.

2.2.9. 求证:

(1) 若 R 是主理想整环, 则 R 的每个同态像也是主理想整环.

(2) $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ $(m \geqslant 1)$ 是主理想整环.

2.2.10. 环 $\mathbb{Z}/3\mathbb{Z}$ 与环 $\mathbb{Z}/6\mathbb{Z}$ 的子环 $2\mathbb{Z}/6\mathbb{Z}$ 是否同构?

2.2.11. 设 $I_1, \cdots, I_n, \cdots$ 均是环 R 中的理想, 并且 $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$. 求证集合 $\bigcup\limits_{i=1}^{\infty} I_n$ 也是环 R 的理想.

2.2.12*. 求证 $T = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{Z} \right\}$ 是环 $M_2(\mathbb{Z})$ 的子环; 试决定环 T 的所有理想.

§3 同态的应用

2.3.1. 设 R 为无零因子环 (未必有单位元) 且满足 $pr = 0$, $\forall\, r \in R$, 其中 p 为素数. 能否将 R 嵌到一个无零因子的含幺环 S 中, 使得 S 的特征为 p?

2.3.2. 设 D 为整环, m 和 n 为互素的正整数, $a, b \in D$. 如果 $a^m = b^m$, $a^n = b^n$, 求证 $a = b$.

2.3.3. 设 R_i $(i \in I)$ 是一个非空的环族, $R = \prod\limits_{i \in I} R_i$. 求证:

(1) R 为含幺环 $\Longleftrightarrow$ 每个 R_i 均为含幺环.

(2) R 为交换环 $\Longleftrightarrow$ 每个 R_i 均为交换环.

(3) $x = (x_i)$ 是 R 中单位 $\Longleftrightarrow$ 每个 x_i 均为 R_i 中单位.

(4) 若 R 为含幺环且 I 有限, 则 R 中理想 A 均形如 $I = \prod\limits_{i \in I} A_i$, 其中每个 A_i 是 R_i 中理想.

2.3.4. 设 S, R_i $(i \in I)$ 均为环, $R = \prod\limits_{i \in I} R_i$, $\pi_i: R \longrightarrow R_i (i \in I)$ 为正则投射, $\varphi_i : S \longrightarrow R_i$ $(i \in I)$ 均是环的同态. 求证存在唯一的环同态 $\varphi : S \longrightarrow R$, 使得对于每个 $i \in I$, 均有 $\pi_i \varphi = \varphi_i$.

2.3.5. 设 R_i $(i \in I)$ 均为环, 求证:

(1) $\bigoplus\limits_{i \in I} R_i = \{(x_i) \in \prod\limits_{i \in I} R_i \mid$ 只有有限多个 $x_i \neq 0\}$ 是 $\prod\limits_{i \in I} R_i$ 的子环. $\bigoplus\limits_{i \in I} R_i$ 叫做环 R_i $(i \in I)$ 的直和.

(2) 设 S 为环, 对于每个 $i \in I$, $\varphi_i: R_i \longrightarrow S$ 均为环同态, $\tau_i : R_i \longrightarrow \bigoplus\limits_{i \in I} R_i$

是正则嵌入. 则存在唯一的环同态 $\varphi: \bigoplus_{i\in I} R_i \longrightarrow S$, 使得 $\varphi_i = \varphi \cdot \tau_i$.

2.3.6. 设 $I_1, \cdots, I_n$ 是环 R 的理想, 并且

(1) $I_1 + \cdots + I_n = R$;

(2) 对于每个 i $(1 \leqslant i \leqslant n)$, $I_i \bigcap (I_1 + \cdots + I_{i-1} + I_{i+1} + \cdots + I_n) = (0)$.

求证 $R \cong \bigoplus_{i=1}^{n} I_i$.

2.3.7. 环 R 中元 e 叫做幂等元, 如果 $e^2 = e$. 如果 e 又属于环 R 的中心, 则称 e 为中心幂等元.

设 R 是含幺环, e 为 R 的中心幂等元. 求证:

(1) $1 - e$ 也是中心幂等元.

(2) eR 和 $(1-e)R$ 均是 R 的理想, 并且 $R \cong eR \times (1-e)R$.

2.3.8. 环 R 中幂等元 e_1, e_2 称为正交的, 如果 $e_1e_2 = 0 = e_2e_1$. 设 $R, R_1, \cdots, R_n$ 都是含幺环, 则下列两个条件等价:

(1) $R \cong R_1 \times \cdots \times R_n$;

(2) R 具有两两正交的中心幂等元 $e_1, \cdots, e_n$, 使得 $e_1 + \cdots + e_n = 1_R$, 并且 $e_iR \cong R_i$ $(1 \leqslant i \leqslant n)$.

2.3.9*. 设 R 是含幺交换环, $P_1, \cdots, P_m$ 为 R 的素理想而 A 为 R 的理想. 如果 $A \subseteq P_1 \bigcup \cdots \bigcup P_m$, 则必存在某个 i $(1 \leqslant i \leqslant m)$, 使得 $A \subseteq P_i$.

2.3.10. 试证: 含幺交换有限环 R 的素理想 I 必是极大理想.

2.3.11. 设 P 是含幺交换环 R 的素理想, $A_1, \cdots, A_n$ 是 R 的理想. 如果 $P = \bigcap_{1\leqslant i\leqslant n} A_i$, 则 P 必等于某个 A_i.

2.3.12. 设 $f: R \longrightarrow S$ 是环的满同态, $K = \operatorname{Ker} f$. 求证:

(1) 若 P 是 R 的素理想并且 $P \supseteq K$, 则 $f(P)$ 也是 S 的素理想.

(2) 若 Q 是 S 的素理想, 则 $f^{-1}(Q) = \{a \in R \mid f(a) \in Q\}$ 也是 R 的素理想.

(3) S 中素理想与 R 中包含 K 的素理想是一一对应的.

将素理想改成极大理想则以上三个论断也成立.

2.3.13. 设 I 是环 R 的理想. 求证 R/I 中素理想均可写成形式 P/I, 其中 P 是 R 中素理想而且包含 I.

将素理想改成极大理想则此论断也成立.

2.3.14. 设 $m \geqslant 2$, 试决定环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 的全部素理想和极大理想.

2.3.15. 设环 R 的加法群同构于有理数加法群 $(\mathbb{Q}, +)$, 而乘法则定义为 $ab = 0,\ \forall\, a, b \in R$. 求证 R 没有素理想和极大理想.

2.3.16. (1) 设 R 是含幺环, 则 R 的极大理想均为素理想.

(2) 设 R 是主理想整环, 则 R 的任一非零素理想均为极大理想.

(3) 设 F 为域, 试问 $F[x]$ 中哪些理想是素理想和极大理想?

2.3.17. 试证: 有单位元的非零环 R 的任一真理想必包含于某一极大理想. 特别地, R 有极大理想 (从而有素理想).

§4 各 类 整 环

2.4.1. (1) 设 R 为整环. 若 $\langle p \rangle$ 是 R 的非零极大理想, 则 p 为不可约元.

(2) 设 R 为主理想整环. 若 p 为不可约元, 则 $\langle p \rangle$ 也是 R 的极大理想.

2.4.2. 设 R 为整环, 则 p 为素元当且仅当 $\langle p \rangle$ 是 R 的非零素理想.

2.4.3. (1) 设 R 为整环. 若 p 为素元, 则 p 为不可约元.

(2) 设 R 为主理想整环. 若 p 为不可约元, 则 p 为素元.

2.4.4. 设 a 为主理想整环 D 中的非零元. 求证: 若 a 为素元, 则 $D/\langle a \rangle$ 为域; 若 a 不是素元, 则 $D/\langle a \rangle$ 不是整环.

2.4.5. 设 R 为整环, $a, b \in R - \{0\},\ a \sim b$ (即 a 与 b 相伴). 求证:

(1) 若 a 为不可约元, 则 b 也为不可约元.

(2) 若 a 为素元, 则 b 也为素元.

2.4.6. 设 R 为 UFD, a, b, c 为 R 中非零元. 求证:

(1) $ab \sim (a, b)[a, b]$;

(2) 若 $a \mid bc,\ (a, b) = 1$, 则 $a \mid c$.

2.4.7. 设 R 为 PID, 求证:

(1) $\langle a \rangle \bigcap \langle b \rangle = \langle [a, b] \rangle$; 并且 $\langle a \rangle \bigcap \langle b \rangle = \langle a \rangle \langle b \rangle \Longleftrightarrow (a, b) = 1$.

(2) 方程 $ax + by = c$ 在 R 中有解 (x, y) 的充分条件是 $(a, b) \mid c$.

2.4.8. 如果 D 为整环但不是域, 则 $D[x]$ 不是主理想整环. 特别地, $\mathbb{Z}[x]$ 不

是 PID.

2.4.9. 证明 $\mathbb{Z}[\sqrt{-2}\,]$ 是 ED, 从而是 UFD. 而 $\mathbb{Z}[\sqrt{-3}\,]$ 不是 UFD.

2.4.10. 设 D 是 PID, E 为整环, 并且 D 是 E 的子环, $a, b \in D - \{0\}$. 如果 d 是 a 和 b 在 D 中的最大公因子, 证明 d 也是 a 和 b 在 E 中的最大公因子.

2.4.11. 求 50 和 $19+9i$ 在 $\mathbb{Z}[i]$ 中的最大公因子.

2.4.12*. 设 $a+bi \in \mathbb{Z}[i]$, 且 $a^2+b^2=p$, p 为素数, 则 $\mathbb{Z}[i]/\langle a+bi\rangle \cong \mathbb{Z}_p$.

§5 多 项 式 环

2.5.1. 试决定环 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 的自同构群.

2.5.2. 如果 $c_0, \cdots, c_n$ 是整环 D 中两两相异的 $n+1$ 个元, $d_0, \cdots, d_n$ 是 D 中任意 $n+1$ 个元, 求证:

(1) 在 $D[x]$ 中至多存在一个次数 $\leqslant n$ 的多项式 $f(x)$, 使得 $f(c_i) = d_i (0 \leqslant i \leqslant n)$.

(2) 如果 D 为域, 则 (1) 中所述的多项式是存在的.

2.5.3. $2x+2$ 在 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 中是否为不可约元? x^2+1 在 $\mathbb{R}[x]$ 和 $\mathbb{C}[x]$ 中是否为不可约元?

2.5.4. 设 D 和 E 为整环, $D \subseteq E$, $f(x) \in D[x]$, c 是 $f(x)$ 在 E 中的一个根. 利用形式微商确定根 c 的重数.

2.5.5. 设 F 是域, $f(x) \in F[x]$, $c_1, \cdots, c_m$ 是 $f(x)$ 在 F 中两两相异的根, 并且根 c_i 的重数为 $\lambda_i, i = 1, \cdots, m$. 求证 $\lambda_1 + \cdots + \lambda_m \leqslant \deg f$.

2.5.6. 设 $f = \sum u_i x^i \in \mathbb{Z}[x]$ 为首 1 多项式, p 为素数, 以 $\overline{a}$ 表示 $a \in \mathbb{Z}$ 在环的自然同态 $\mathbb{Z} \longrightarrow \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 之下的像, 而令 $\overline{f}(x) = \sum \overline{u}_i x^i \in \mathbb{Z}_p[x]$. 求证:

(1) 如果对某个素数 p, $\overline{f}(x)$ 在 $\mathbb{Z}_p[x]$ 中不可约, 则 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约.

(2) 如果 $f(x)$ 不是 $\mathbb{Z}[x]$ 中首 1 多项式, 试问 (1) 中的结论是否成立?

2.5.7. 设 D 为 UFD, F 为 D 的商域, $f(x)$ 为 $D[x]$ 中首 1 多项式. 求证: $f(x)$ 在 $F[x]$ 中的每个首 1 多项式因子必然属于 $D[x]$.

2.5.8. 设 R 是含幺交换环, $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. 则 $f \in U(R[x]) \Longleftrightarrow a_0 \in U(R)$, 并且 $a_1, \cdots, a_n$ 均是 $R[x]$ 中的幂零元.

2.5.9*. (Eisenstein 判别法的推广) 设 $f(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}[x]$, $\deg f=n$. $(a_0,a_1,\cdots,a_n)=1$. 如果存在素数 p 和整数 k $(0<k\leqslant n)$, 使得

$$p\nmid a_k,\quad p\mid a_i\quad(0\leqslant i\leqslant k-1),\quad p^2\nmid a_0,$$

求证 $f(x)$ 在 $\mathbb{Z}[x]$ 中必存在次数 $\geqslant k$ 的不可约因子.

2.5.10. 将 x^n-1 $(3\leqslant n\leqslant 10)$ 在 $\mathbb{Z}[x]$ 中作素因子分解.

2.5.11. 设 D 为整环, $f(x)\in D[x]$, $c\in D$, $g(x)=f(x+c)\in D[x]$. 求证:
(1) $f(x)$ 在 $D[x]$ 中本原 $\Longleftrightarrow g(x)$ 在 $D[x]$ 中本原.
(2) $f(x)$ 在 $D[x]$ 中不可约 $\Longleftrightarrow g(x)$ 在 $D[x]$ 中不可约.

2.5.12. 设 R 为任意环, 定义集合

$$R[[x]]=\left\{\sum_{n=0}^{\infty}a_nx^n\mid a_n\in R,\ n=0,1,2,\cdots\right\},$$

每个元 $\sum_{n=0}^{\infty}a_nx^n$ 叫做 R 上关于 x 的形式幂级数. 定义

$$\sum a_nx^n+\sum b_nx^n=\sum(a_n+b_n)x^n,$$
$$(\sum a_nx^n)(\sum b_nx^n)=\sum c_nx^n,$$

其中 $c_n=\sum_{i+j=n}a_ib_j$, $n=0,1,2,\cdots$. 求证:

(1) $R[[x]]$ 对于上述加法和乘法形成环, 叫做环 R 上关于 x 的形式幂级数环.

(2) 若 R 有幺元 1, 则 1 也是 $R[[x]]$ 的幺元. 若 R 为交换环, 则 $R[[x]]$ 也是交换环.

(3) 多项式环 $R[x]$ 自然看成是 $R[[x]]$ 的子环.

(4) 设 R 是含幺交换环, $f(x)=\sum_{n=0}^{\infty}a_nx^n\in R[[x]]$. 则

$$f(x)\in U(R[[x]])\Longleftrightarrow a_0\in U(R).$$

(5) 若 a_0 在 R 中不可约, 则 $f(x)$ 在 $R[[x]]$ 中不可约.

2.5.13. 设 F 是域, 求证:

(1) 环 $F[[x]]$ 只有一个极大理想 M, 并且 $F[[x]]$ 中全部理想为 M^n ($n = 0, 1, 2, \cdots$), 其中规定 $M^0 = F[[x]]$. 并且当 $n \neq m$ 时, $M^n \neq M^m$.

(2) $F[[x]]$ 为主理想整环, 从而为 UFD.

2.5.14. $x + 1$ 是否为环 $\mathbb{Z}[x]$ 和 $\mathbb{Z}[[x]]$ 中单位? $x^2 + 3x + 2$ 是否为 $\mathbb{Z}[x]$ 和 $\mathbb{Z}[[x]]$ 中不可约元?

2.5.15*. 设 $f(x)$ 是 $\mathbb{Q}[x]$ 中奇次不可约多项式, α 和 β 是 $f(x)$ 在 $\mathbb{Q}$ 的某个扩域中两个不同的根. 求证 $\alpha + \beta \notin \mathbb{Q}$.

2.5.16*. 设 k 是域, $f(x_1, x_2)$ 和 $g(x_1, x_2)$ 是 $k[x_1, x_2]$ 中两个互素的多项式. 求证在 k 的任意扩域中 $f(x_1, x_2) = 0$ 和 $g(x_1, x_2) = 0$ 均只有有限多公共解 (x_1, x_2).

第 3 章　域　论

§1　域的扩张

3.1.1. 设 K/F 为域的扩张, 求证:

(1) 若 $[K:F]$ 是素数, 则 $K=F(u)$, 其中 u 是 K 中任一不属于 F 的元.

(2) 若 $u\in K$ 是 F 上奇次代数元, 则 $F(u)=F(u^2)$.

3.1.2. 求元 a 在域 F 上的极小多项式, 其中

(1) $a=\sqrt{2}+\sqrt{3}$, $F=\mathbb{Q}(\sqrt{6})$;

(2) $a=\sqrt{2}+\sqrt{3}$, $F=\mathbb{Q}(\sqrt{2})$;

(3) $a=\sqrt{2}+\sqrt{3}$, $F=\mathbb{Q}$.

3.1.3. 设 u 属于 F 的某个扩域, 并且 u 在 F 上代数. 如果 $f(x)$ 为 u 在 F 上的极小多项式, 则 $f(x)$ 必为 $F[x]$ 中不可约多项式. 反之, 若 $f(x)$ 是 $F[x]$ 中首 1 不可约多项式, 并且 $f(u)=0$, 则 $f(x)$ 为 u 在 F 上的极小多项式.

3.1.4. 设 u 是域 F 的某扩域中的元, 并且 x^n-a 是 u 在 F 上的极小多项式. 对于 $m|n$, 求 u^m 在域 F 上的极小多项式.

3.1.5. 设 K/F 为域的代数扩张, D 为整环并且 $F\subseteq D\subseteq K$, 求证 D 为域.

3.1.6. 设 K/F 为域扩张, $a\in K$. 若 $a\in F(a^m)$, $m>1$, 则 a 在 F 上代数.

3.1.7. 设 u 是多项式 x^3-6x^2+9x+3 的一个实根.

(1) 求证 $[\mathbb{Q}(u):\mathbb{Q}]=3$;

(2) 将 u^4, $(u+1)^{-1}$, $(u^2-6u+8)^{-1}$ 表示成 $1,\ u,\ u^2$ 的 $\mathbb{Q}-$ 线性组合.

3.1.8. 设 p 为素数, 求扩张 $\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}})/\mathbb{Q}$ 和 $\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{8}})/\mathbb{Q}$ 的次数.

3.1.9. 设 x 是 $\mathbb{Q}$ 上的超越元, $u=x^3/(x+1)$. 求 $[\mathbb{Q}(x):\mathbb{Q}(u)]$.

3.1.10. (1) 设 K/F 是域的扩张, 求证 $M=\{a\in K\mid a$ 在 F 上代数 $\}$ 为 K 的一个包含 F 的子域 (称作 F 在 K 中的代数闭包).

(2) 设 K/F 为域的扩张, K 是代数封闭域. 则 (1) 中的域 M 是 F 的一个代数闭包 (即 M 是代数封闭域且 M/F 是代数扩张).

3.1.11. 设 M/F 为域的扩张, M 中的元 u,v 分别是 F 上的 m 次和 n 次代数元. $K=F(u)$, $E=F(v)$. 求证:

(1) $[KE:F]\leqslant mn$;

(2) 如果 $(m,n)=1$, 则 $[KE:F]=mn$.

3.1.12. 试证关于域 K 的以下四个命题是等价的:

(1) K 为代数封闭域;

(2) $K[x]$ 中每个次数 $\geqslant 1$ 的多项式在 $K[x]$ 中均可表示成一些一次多项式的乘积;

(3) $K[x]$ 中每个次数 $\geqslant 1$ 的多项式在 K 中均有根;

(4) $f(x)$ 为 $K[x]$ 中不可约元 $\Longleftrightarrow \deg f(x)=1$.

3.1.13. 设 $K=\mathbb{Q}(\alpha)$ 为 $\mathbb{Q}$ 的单扩张, 其中 α 在 $\mathbb{Q}$ 上代数. 求证 $|\operatorname{Aut}(K)|\leqslant [K:\mathbb{Q}]$.

3.1.14. 给出域扩张 K/F 的例子, 使得 $K=F(u,v)$, u 和 v 均是 F 上超越元, 但是 $K\ncong F(x_1,x_2)$, 其中 $F(x_1,x_2)$ 表示 F 上两个独立的不定元 x_1, x_2 的有理函数域.

3.1.15 . 如果 u 是 K 上关于文字 $x_1,\cdots,x_n$ 的有理函数 (即 $u\in K(x_1,\cdots,x_n)$), 但是 $u\notin K$, 求证 u 在 K 上超越.

3.1.16 . 设 K 是域, x 是 K 上的超越元, $u\in K(x)$, $u\notin K$. 求证 x 在域 $K(u)$ 上代数.

3.1.17. 设 E/F 是域的扩张, 如果对每个元 $\alpha\in E$, $\alpha\notin F$, α 在 F 上均是超越元, 则称 E/F 为纯超越扩张. 求证:

(1) $F(x)/F$ 是纯超越扩张.

(2) 对于任意域扩张 E/F, 求证存在唯一的中间域 M, 使得 E/M 为纯超越扩张, 而 M/F 为代数扩张.

§2 分 裂 域

3.2.1. 写出二元域 $\mathbb{Z}_2=\mathbb{Z}/2\mathbb{Z}$ 上一个二次不可约多项式 $f(x)$. 将 $f(x)$ 的一个根添加到 $\mathbb{Z}_2$ 中, 写出域 $\mathbb{Z}_2(u)$ 的全部元以及它们的加法表和乘法表.

3.2.2. 设 $f(x)$ 是 $K[x]$ 中多项式, $\deg f(x)=n\geqslant 1$. 求证存在 K 的某个扩域 E, 使得 $[E:K]\leqslant n!$, 并且 $f(x)$ 在 $E(x)$ 中分解成 n 个一次多项式之积.

3.2.3*. (1) 设 n 是正整数, 域 F 的特征为零或与 n 互素. 则多项式 $x^n-1\in F[x]$ 在 K 中的根集 G 是 n 阶循环群, 其中 K 是 x^n-1 在 F 上的分裂域的任

一扩域.

(2) 域的乘法群的任一有限子群均是循环群.

3.2.4. 设 F 是特征不为 2 的域, 求证 F 的每个二次扩张均有形式 $F(\sqrt{d})$, $d \in F$. 如果 $\operatorname{char} F = 2$, 结论是否成立?

3.2.5. 设 F 为域, $c \in F$, p 为素数. 求证: $x^p - c$ 在 $F[x]$ 中不可约 $\Longleftrightarrow$ $x^p - c$ 在 F 中无根.

3.2.6*. 设 F 是特征 p 域, p 为素数, $c \in F$.

(1) 求证: $x^p - x - c$ 在 $F[x]$ 中不可约 $\Longleftrightarrow$ $x^p - x - c$ 在 F 中无根.

(2) 如果 $\operatorname{char} F = 0$, 试问 (1) 中结论是否仍旧成立?

3.2.7*. 设 F 为域, E 是 $F(x)$ 中 n 次多项式 $f(x)$ 在 F 上的分裂域. 求证 $[E : F] \mid n!$.

3.2.8. 设 E 为 $x^8 - 1$ 在 $\mathbb{Q}$ 上的分裂域. 求 $[E : \mathbb{Q}]$, 并决定 Galois 群 $\operatorname{Gal}(E/\mathbb{Q})$.

§3　有限域的结构

3.3.1. (1) 列出 $\mathbb{Z}_2$ 上全部次数小于 5 的不可约多项式.

(2) 列出 $\mathbb{Z}_3$ 上全部 2 次不可约多项式.

3.3.2. 构作一个 8 元域, 并指出它的加法法则和乘法法则.

3.3.3. 给出 9 元域 $\mathbb{Z}_3(u)$ 和 9 元域 $\mathbb{Z}_3(v)$ 之间的一个同构, 其中 u 和 v 分别是 $\mathbb{Z}_3[x]$ 中多项式 $x^2 + 1$ 和 $x^2 + x + 2$ 的根.

3.3.4. (1) p^n 元域 $F = \mathbb{Z}_p(u)$ 中的 u 是否一定是乘法循环群 F^* 的生成元?

(2) 若 n 和 $2^n - 1$ 均是素数, 2^n 元域 $\mathbb{Z}_2(u)$ 中的元 u 是否一定是其乘法循环群的生成元?

3.3.5. $F_q[x]$ 中 n 次首 1 不可约多项式 $f(x)$ 称为 $F_q[x]$ 中的 n 次本原多项式, 如果 $f(x)$ 的某一根 u 是域 $F_q(u)$ 的乘法循环群的生成元.

(1) 证明 $x^4 + x + 1$ 为 $\mathbb{Z}_2[x]$ 中本原多项式.

(2) 列出 16 元域 $\mathbb{Z}_2(u)$ 中 (唯一的) 4 元子域 F_4 的全部元, 这里 u 是 $x^4 + x + 1 \in \mathbb{Z}_2[x]$ 的一个根.

(3) 求出 u 在 4 元域上的极小多项式.

3.3.6. (1) 证明 $x^4+x^3+x^2+x+1$ 为 $\mathbb{Z}_2[x]$ 中不可约多项式但不是本原多项式.

(2) 令 u 为 $x^4+x^3+x^2+x+1\in\mathbb{Z}_2[x]$ 的一个根, 试问 $F_{16}=\mathbb{Z}_2(u)$ 中哪些元是 F_{16} 的乘法群的生成元?

3.3.7. 设 F 为 q 元域, $q=p^n$, p 为素数, H 是 $\mathrm{Aut}(F)$ 的 m 阶子群, $K=\{a\in F\mid$ 对每个 $\alpha\in H$, $\alpha(a)=a\}$. 求证:

(1) $m|n$;

(2) K 是 F 中唯一的 $p^{n/m}$ 元子域.

3.3.8. 求证:

(1) $F_{p^n}\supseteq F_{p^m}\Longleftrightarrow m/n$.

(2) 设 $F_{p^n}\supseteq F_{p^m}$, 令 $G=\{\sigma\in\mathrm{Aut}(F_{p^n})\mid$ 对每个 $a\in F_{p^m}$, $\sigma(a)=a\}$, 则 G 是 n/m 阶循环群.

3.3.9. 求证: 代数封闭域必是无限域.

3.3.10*. 求证: 域 F 是有限域当且仅当 F 的乘法群 F^* 是循环群.

3.3.11*. 设 $a,b\in F_{2^n}$, n 是奇数. 若 $a^2+b^2+ab=0$, 则 $a=b=0$.

3.3.12*. 设 F 是有限域, $a,b\in F^*$. 求证: 对每个 $c\in F$, 方程 $ax^2+by^2=c$ 在域 F 中均有解 (x,y).

特别地, 有限域的任意元均可写成两个元的平方和.

3.3.13*. 设 $F=F_q$, $(n,q)=1$, E 为 x^n-1 在 F 上的分裂域. 求证: $[E:F]$ 是满足 $n|(q^k-1)$ 的最小正整数 k.

3.3.14*. 设 $c\in F_q^*$, m 为正整数. 则

(1) 方程 $x^m=c$ 在 F_q 中有解当且仅当 $c^{\frac{q-1}{(q-1,m)}}=1$.

(2) 若 $x^m=c$ 在 F_q 中有解, 它恰有 $(q-1,m)$ 个解.

(3) F_q^* 中恰有 $\dfrac{q-1}{(q-1,m)}$ 个元 c, 使得方程 $x^m=c$ 在 F_q 中有解.

(4) F_q 中任一元均是 F_q 中某一元的 m 次幂当且仅当 $(q-1,m)=1$.

3.3.15*. 设 q 为素数幂, 求证:

(1) 有限域 F_q 的所有元之和为零, 其中 $q\neq 2$.

(2) 设 $q-1=ds$, d, s 均为正整数且 $s>1$, 则 F_q^* (唯一) 的 s 阶子群的所有元之和为零.

(3) 设 m 为正整数, 则

$$\sum_{a\in F_q} a^m = \begin{cases} -1, & (q-1)\mid m, \\ 0, & (q-1)\nmid m. \end{cases}$$

§4 有限域上的不可约多项式

3.4.1. 对每个正整数 n, $F_q[x]$ 中必存在 n 次不可约多项式.

3.4.2*. 多项式 $x^{q^n}-x$ 是 $F_q[x]$ 中所有次数整除 n 的不可约首 1 多项式的乘积.

特别地, F_q 上任一 n 次不可约首 1 多项式均是 $x^{q^n}-x$ 的次数最高的不可约因子.

3.4.3. 设 $f(x)$ 是 $F_q[x]$ 中 n 次首 1 不可约多项式, u 为 $f(x)$ 的一个根. 则

(1) $f(x)$ 共有 n 个彼此不同的根: $u,\ u^q,\cdots,\ u^{q^{n-1}}$.

(2) n 是使得 $u^{q^n-1}=1$ 的最小正整数.

(3) 设 l 是 u 的乘法阶, 则 n 是使得 $l\mid q^n-1$ 的最小正整数; 且 $f(x)$ 的任一根的乘法阶均为 l.

3.4.4. 求证: x^5-x+1 是 $\mathbb{Z}_3[x]$ 中的本原多项式.

3.4.5*. (1) 设 $f(x)$ 是 $F_q[x]$ 中 n 次首 1 不可约多项式. 若 $f(x)$ 的一个根 u 为域 $F_q(u)$ 的乘法循环群 $F_q^*(u)$ 的生成元, 则 $f(x)$ 的每个根也都是 $F_q^*(u)$ 的生成元.

(2) $F_q[x]$ 中 n 次首 1 不可约多项式 $f(x)$ 称为 $F_q[x]$ 中的 n 次本原多项式, 如果 $f(x)$ 的某一根 u 是域 $F_q(u)$ 的乘法循环群的生成元. 证明 $F_q[x]$ 中共有 $\dfrac{\varphi(q^n-1)}{n}$ 个 n 次本原多项式, 其中 $\varphi(n)$ 是 Euler 函数 (即 $\varphi(n)$ 是小于 n 的正整数中与 n 互素的正整数的个数).

3.4.6*. 求证: 当 $n\geqslant 3$ 时, $x^{2^n}+x+1$ 是 $\mathbb{Z}_2[x]$ 中可约多项式.

3.4.7*. Möbius 函数 $\mu:\ \mathbb{N}\longrightarrow\{0,1,-1\}$ 定义如下:

$$\mu(n)=\begin{cases} 1, & \text{若 } n=1, \\ 0, & \text{若 } n \text{ 被素数的平方整除}, \\ (-1)^r, & \text{若 } n \text{ 是 } r \text{ 个互异的素数之积}. \end{cases}$$

则

(1) μ 是积性函数, 即: 若 n 和 m 是互素的正整数, 则 $\mu(mn)=\mu(m)\mu(n)$.

(2) 对于任一正整数 n 有

$$\sum_{d|n}\mu(d)=\sum_{d|n}\mu\left(\frac{n}{d}\right)=\begin{cases}1, & n=1,\\ 0, & n>1.\end{cases}$$

(3) (Möbius 反演律) 设 H 和 h 均为正整数集 $\mathbb{N}$ 到 Abel 群 G 的映射 (G 的运算用加法表示). 若

$$H(n)=\sum_{d|n}h(d),\quad \forall\, n\in\mathbb{N},$$

则

$$h(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)H(d)=\sum_{d|n}\mu(d)H\left(\frac{n}{d}\right),\quad \forall\, n\in\mathbb{N};$$

反之亦然.

3.4.8*. 求证: 有限域 F_q 上 n 次首 1 不可约多项式的个数 $N_q(n)$ 为

$$N_q(n)=\frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d.$$

§5 有限域上的线性代数

3.5.1. 以下方阵的集合

$$\left\{\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}\ \middle|\ a,b,c\in F_q\right\}$$

对于矩阵的乘法作成 q^3 阶非 Abel 群.

3.5.2*. 求有限域 F_q 上 m $(m\geqslant 1)$ 次一般线性群 $GL_m(F_q)$ 的阶.

3.5.3*. 求有限域 F_q 上 m $(m\geqslant 2)$ 次特殊线性群 $SL_m(F_q)$ 的阶.

3.5.4*. 证明有限域 F_q 上 m $(m\geqslant 1)$ 维线性空间 V 有 s 组 (两两不同的) 基, 其中

$$s=\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})}{m!}.$$

3.5.5. 有限域 F_{p^n} 作为其子域 F_{p^d} 上的线性空间, 有多少组 (两两不同的) 基?

3.5.6*. 求证: 有限域 F_q 上 m $(m \geqslant 1)$ 维线性空间 V 的 t $(1 \leqslant t \leqslant m)$ 维子空间的个数为

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}.$$

3.5.7. 设 q 是非零实数且非单位根, 证明

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})} = \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{m-t-1})}{(q^{m-t}-1)(q^{m-t}-q)\cdots(q^{m-t}-q^{m-t-1})}.$$

由此即知: 有限域 F_q 上 m $(m \geqslant 1)$ 维线性空间 V 的 t $(1 \leqslant t \leqslant m-1)$ 维子空间的个数等于 V 的 $m-t$ 维子空间的个数.

3.5.8. 将有限域 F_{q^m} 看成其子域 F_q 上的 m 维线性空间, 则

(1) 有限域 F_{q^m} 有多少个 t $(1 \leqslant t \leqslant m)$ 维 F_q- 子空间?

(2) 有限域 F_{q^m} 有多少组含有 t $(1 \leqslant t \leqslant m)$ 个元的 F_q- 线性无关向量组?

3.5.9*. 设 G 为 Galois 群 $\mathrm{Gal}(F_{q^n}/F_q)$. 对于每个 $a \in F_{q^n}$, 令

$$T(a) = \sum_{\sigma \in G} \sigma(a), \quad N(a) = \prod_{\sigma \in G} \sigma(a).$$

求证:

(1) $T:\ F_{q^n} \longrightarrow F_q$ 是 F_q- 线性满射.

(2) $N:\ F_{q^n}^* \longrightarrow F_q^*$ 是乘法群的满同态.

3.5.10*. 求群 $G = GL_n(\mathbb{Z}_p)$ 的 Sylow p- 子群的个数.

3.5.11*. **Dedekind 引理**: 设 E 是任一域, 则 $\mathrm{Aut}(E)$ 的任一有限子集是 E- 线性无关的, 即对于 $\mathrm{Aut}(E)$ 的任一有限子集 Ω, 如果 $\sum_{\sigma \in \Omega} f(\sigma)\sigma = 0$, 其中 $f(\sigma) \in E$, $\forall\ \sigma \in \Omega$, 则 $f(\sigma) = 0$, $\forall\ \sigma \in \Omega$.

§6 可分扩张

3.6.1. 设 F 是特征为 0 的域, $f(x)$ 为 $F[x]$ 中正次数首 1 多项式, $d(x) = (f(x), f'(x))$, 其中 $f'(x)$ 是 $f(x)$ 的导数. 求证: $g(x) = f(x)/d(x)$ 和 $f(x)$ 有同样的根, 并且 $g(x)$ 无重根.

3.6.2. 设 F 是特征为 p 的域 (p 为素数), $f(x)$ 为 $F[x]$ 中不可约多项式. 求证: $f(x)$ 的所有根均有相同的重数, 且这个公共重数有形式 p^e $(e \geqslant 0)$.

3.6.3. 设 F 是特征为 p 的域 (p 为素数), E/F 为代数扩张. 求证: 对每个 $\alpha \in E$ 均存在整数 $n \geqslant 0$, 使得 α^{p^n} 在 F 上可分.

3.6.4. 设有域扩张 K/F, $\operatorname{char} F = p$, $\alpha \in K$. 则 α 是 F 上的可分元当且仅当 $F(\alpha) = F(\alpha^p)$.

3.6.5*. 设 α 在 F 上可分, β 在 $F(\alpha)$ 上可分, 则 β 在 F 上可分.

3.6.6*. (1) 设 E/F 为代数扩张, S 是 E 的子集. 证明: $F(S)/F$ 是可分扩张当且仅当 S 中元在 F 上都是可分的.

(2) 若 α, β 在 F 上可分, 则 $\alpha \pm \beta, \alpha\beta, \dfrac{\alpha}{\beta}$ $(\beta \neq 0)$ 均在 F 上可分.

(3) F 上可分多项式在 F 上的分裂域在 F 上可分.

(4) 若 E/K 和 K/F 为可分扩张, 则 E/F 为可分扩张; 反之亦然.

3.6.7*. **同构延拓定理的强形式** 设 $\sigma: F \longrightarrow F'$ 是域同构, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 是 $F[x]$ 中的正次数多项式, E 和 E' 分别是 $f(x)$ 在 F 上和 $f^{\sigma}(x) = \sigma(a_n)x^n + \sigma(a_{n-1})x^{n-1} + \cdots + \sigma(a_1)x + \sigma(a_0)$ 在 F' 上的分裂域. 则 σ 可延拓成域同构 $E \longrightarrow E'$; 这种延拓的个数 m 满足 $1 \leqslant m \leqslant [E:F]$.

而且 $m = [E:F]$ 当且仅当 $f(x)$ 是 F 上的可分多项式.

3.6.8. 设 $E = F_p(x, y)$, $F = F_p(x^p, y^p)$, 其中 F_p 为 p 元域, x, y 是 F_p 上的超越元. 求证:

(1) $[E:F] = p^2$.

(2) E/F 不是单扩张.

(3) E/F 有无限多个中间域.

3.6.9. (1) 若 E/F 为代数扩张, F 为完全域, 则 E 也为完全域.

(2) 若 E/F 为有限扩张, E 为完全域, 问 F 是否也为完全域?

(3) 若 E/F 为有限生成扩张 (不必为代数扩张), E 为完全域, 问 F 是否也为完全域?

(4) 若 E/F 为有限扩张, E 为完全域, 问 F 是否也为完全域?

(5) 若 E/F 为代数扩张 (不必为有限扩张), E 为完全域, 问 F 是否也为完全域?

§7 正 规 扩 张

3.7.1. 设 $E = \mathbb{Q}(\alpha)$, 其中 $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$. 求证:

(1) $\alpha^2 - 2$ 也是 $x^3 + x^2 - 2x - 1 = 0$ 的根.

(2) $E/\mathbb{Q}$ 是正规扩张.

3.7.2. 设 E/F 和 K/F 均是正规扩张, 求证: EK/F 也是正规扩张.

3.7.3. 域的二次扩张 E/F 必是正规扩张. 试决定二次扩张的 Galois 群.

3.7.4. (1) 如果 E/M 和 M/F 均是域的正规扩张, 试问 E/F 是否一定为正规扩张?

(2) 如果 E/F 是正规扩张, M 是它们的中间域, 试问 E/M 和 M/F 是否一定为正规扩张?

3.7.5*. 设 E/F 为有限代数扩张. 求证: E/F 为正规扩张 $\Longleftrightarrow$ 对于 $F[x]$ 中任意不可约多项式 $f(x)$, $f(x)$ 在 $E[x]$ 中的所有不可约因子均有相同的次数.

3.7.6*. 设 E/F 为有限正规扩张, $G = \mathrm{Gal}(E/F)$, M 是 E/F 的中间域. 则 M/F 是正规扩张当且仅当 $\sigma(M) = M$, $\forall\, \sigma \in G$.

第 4 章　Galois 理论

§1　基 本 定 理

4.1.1. 求证:

(1) $\mathrm{Gal}(E/-):\Omega\longrightarrow\Gamma$ 和 $\mathrm{Inv}:\Gamma\longrightarrow\Omega$ 是反序的映射, 即若 $M_1\subseteq M_2$, 则 $\mathrm{Gal}(E/M_1)\supseteq\mathrm{Gal}(E/M_2)$; 若 $H_1\subseteq H_2$, 则 $\mathrm{Inv}(H_1)\supseteq\mathrm{Inv}(H_2)$.

(2) (作用 3 次等于作用 1 次) 对于 $M\in\Omega$, $H\in\Gamma$ 有

$$\mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/M)))=\mathrm{Gal}(E/M),\qquad \mathrm{Inv}(\mathrm{Gal}(E/\mathrm{Inv}(H)))=\mathrm{Inv}(H).$$

4.1.2*. 证明 Artin 引理: 设 K 是域, G 是 K 的自同构群 $\mathrm{Aut}(K)$ 的有限子群. 则有 $[K:\mathrm{Inv}(G)]\leqslant|G|$, 这里 $\mathrm{Inv}(G)=\{\ a\in K\mid\sigma(a)=a,\ \forall\,\sigma\in G\ \}$.

4.1.3*. 证明 Galois 理论基本定理:

(1) $\mathrm{Gal}(E/-):\ \Omega\longrightarrow\Gamma$ 和 $\mathrm{Inv}:\ \Gamma\longrightarrow\Omega$ 是互逆的反序的映射.

(2) H 是 G 的正规子群当且仅当 $\mathrm{Inv}(H)/F$ 是正规扩张. 在这种情况下, 有

$$\mathrm{Gal}(\mathrm{Inv}(H)/F)\cong G/H.$$

4.1.4. 设 $E=\mathbb{Q}(\sqrt{2},\sqrt{3},u)$, $u^2=(9-5\sqrt{3})(2-\sqrt{2})$. 求证 $E/\mathbb{Q}$ 是 Galois 扩张, 并决定 Galois 群 $\mathrm{Gal}(E/\mathbb{Q})$.

4.1.5. 设 $E=\mathbb{C}(t)$ (复数域上有理函数域), σ, $\tau\in\mathrm{Gal}(E/\mathbb{C})$, 其中 $\sigma(t)=\omega t$, $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$, $\tau(t)=t^{-1}$. 求证:

(1) τ 和 σ 生成的群 H 是 $\mathrm{Gal}(E/\mathbb{C})$ 的 6 阶子群.

(2) $\mathrm{Inv}(H)=\mathbb{C}(t^3+t^{-3})$.

4.1.6. 设域 F 的特征为素数 p, $\sigma\in G=\mathrm{Gal}(F(x)/F)$, 其中 $\sigma(x)=x+1$. 令 H 为由 σ 生成的 G 之子群, 求证 $|H|=p$. 试问: $\mathrm{Inv}(H)=?$

4.1.7. 设域 F 的特征为素数 p, $a\in F$. 求证:

(1) x^p-x-a 是 $F[x]$ 中不可约多项式 $\Longleftrightarrow$ 不存在 $c\in F$, 使得 $a=c^p-c$.

(2) 如果 x^p-x-a 在 $F[x]$ 中不可约, 令 α 为 x^p-x-a 的一个根, 求证 $F(\alpha)/F$ 为 Galois 扩张. 试决定 Galois 群 $\mathrm{Gal}(F(\alpha)/F)$.

4.1.8*. 设 L 和 M 均是域 E 的子域. 求证: 如果 $L/(L\bigcap M)$ 为有限 Galois 扩张, 则 LM/M 也为有限 Galois 扩张, 并且 $\mathrm{Gal}(LM/M)\cong\mathrm{Gal}(L/(L\bigcap M))$.

4.1.9. 设 E/F 为有限 Galois 扩张, N 和 M 为中间域, $E \supseteq N \supseteq M \supseteq F$. 并且 N 是 M 在 F 上的正规闭包. 求证:

$$\mathrm{Gal}(E/N) = \bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma \mathrm{Gal}(E/M) \sigma^{-1}.$$

4.1.10. 设 E 为 $x^4 - 2$ 在 $\mathbb{Q}$ 上的分裂域.
(1) 试求出 $E/\mathbb{Q}$ 的全部中间域.
(2) 试问哪些中间域是 $\mathbb{Q}$ 的 Galois 扩张? 哪些域彼此共轭?

4.1.11. 设 $\zeta = \mathrm{e}^{\frac{2\pi\mathrm{i}}{12}}$, 求证 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 是 Galois 扩张. 求 $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. 列出 G 的全部子群和它们对应的 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 的中间域.

4.1.12. 对 $\zeta = \mathrm{e}^{\frac{2\pi}{9}\mathrm{i}}$ 做 4.1.11 题的事情.

4.1.13. 设 n 为大于 2 的整数, $\zeta_n = \mathrm{e}^{\frac{2\pi}{n}\mathrm{i}}$, $\mathbb{R}$ 为实数域. 求证: $\mathbb{Q}(\zeta_n) \bigcap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

4.1.14*. 设 p 为奇素数, $\zeta_p = \mathrm{e}^{\frac{2\pi}{p}\mathrm{i}}$. 求证 $\mathbb{Q}(\zeta_p)$ 有唯一的二次子域 K (即 K 为 $\mathbb{Q}(\zeta_p)$ 的子域并且 $[K : \mathbb{Q}] = 2$). 进而, K 是实二次域 (即 $K \subseteq \mathbb{R}$) $\Longleftrightarrow p \equiv 1 \pmod 4$.

4.1.15. 设 E/F 为有限 Galois 扩张. 如果对任一域 K $(F \subsetneqq K \subseteq E)$, K 对 F 均有相同的扩张次数 $[K : F]$, 则 $[E : F] = p, p$ 为素数.

4.1.16. (1) 求证 $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ 是 Galois 扩张, 并求此扩张的 Galois 群.
(2) 求元 $\sqrt{6} + \sqrt{10} + \sqrt{15}$ 在 $\mathbb{Q}$ 上的极小多项式.
(3) 求证 $\sqrt{6} \in \mathbb{Q}\,(\sqrt{6} + \sqrt{10} + \sqrt{15})$.
(4) 求 $\sqrt{2} + \sqrt{3}$ 在 $\mathbb{Q}\,(\sqrt{6} + \sqrt{10} + \sqrt{15})$ 上的极小多项式.

§2 方程的 Galois 群

4.2.1. 设 F 是特征为 2 的域. 求 $f(x)$ 在 F 上的 Galois 群, 其中
(1) $f(x) = x^3 + x + 1$.
(2) $f(x) = x^3 + x^2 + 1$.

4.2.2. 设 $f(x) \in \mathbb{R}[x]$ 是三次不可约多项式. 求证: $d(f) > 0$ 当且仅当 $f(x)$ 有三个实根; $d(f) < 0$ 当且仅当 $f(x)$ 只有一个实根.

4.2.3. 求 Galois 群 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}(1+\mathrm{i}))/\mathbb{Q})$, 其中 $\mathrm{i} = \sqrt{-1}$.

4.2.4. 设 p 为素数, $a \in \mathbb{Q}$, $x^p - a$ 为 $\mathbb{Q}[x]$ 中不可约多项式. 求 $x^p - a$ 在 $\mathbb{Q}$ 上的 Galois 群.

4.2.5. 决定 $f(x)$ 在 $\mathbb{Q}$ 上的 Galois 群, 其中

(1) $f(x) = x^5 - 6x + 3$.

(2) $f(x) = x^5 - 15x^2 + 9$.

4.2.6. 决定 $f(x)$ 在域 F 上的 Galois 群, 其中

(1) $f(x) = x^4 - 5, \quad F = \mathbb{Q}$.

(2) $f(x) = x^4 - 5, \quad F = \mathbb{Q}(\sqrt{5})$.

(3) $f(x) = x^4 - 5, \quad F = \mathbb{Q}(\sqrt{5}\mathrm{i})$.

(4) $f(x) = x^4 - 10x^2 + 4, \quad F = \mathbb{Q}$.

4.2.7. 设 $n \geqslant 2$ 是正整数, 域 F 的特征为零或与 n 互素, ξ 是 n 次本原单位根, E 是 $f(x) = x^n - 1$ 在 F 上的分裂域. 则

$$\mathrm{Gal}(f(x), F) = \begin{cases} (\mathbb{Z}_n)^*, & \xi \notin F, \\ \{1\}, & \xi \in F, \end{cases}$$

其中 $(\mathbb{Z}_n)^*$ 是 $\mathbb{Z}_n$ 的单位群.

4.2.8. 设 $n \geqslant 2$ 是正整数, 域 F 的特征为零或与 n 互素, ξ 是 n 次本原单位根且 $\xi \in F$, E 是 $f(x) = x^n - a \in F[x]$ 在 F 上的分裂域. 则 $\mathrm{Gal}(f(x), F)$ 是循环群; 且当 $f(x)$ 在 F 上不可约时, $\mathrm{Gal}(f(x), F)$ 是 n 阶循环群.

4.2.9*. 设 p^n (p 为素数, $n \geqslant 1$) 次 Galois 扩张 E/F 的 Galois 群 $\mathrm{Gal}(E/F)$ 是 p^n 阶循环群, L 是 E/F 的中间域且 $[E:L] = p$. 若 $E = L(u)$, 则 $E = F(u)$.

4.2.10*. 设 E/F 是有限次 Galois 扩张, 其 Galois 群 $\mathrm{Gal}(E/F)$ 含有最小子群 A, $L = \mathrm{Inv}(A)$. 若 $E = L(u)$, 则 $E = F(u)$.

4.2.11. 任一有限群均是某个域上可分多项式的 Galois 群.

§3　方程的根式可解性

4.3.1*. 设 p 次 Galois 扩张 E/F 的 Galois 群 $\mathrm{Gal}(E/F)$ 是 p 阶循环群 (p 为素数), 且 F 含有 p 次本原单位根 ξ. 则存在 $d \in E$ 使得 $E = F(d)$, $d^p \in F$. 故 E/F 是根式扩张.

4.3.2*. 设域 F 的特征为零, E 是 F 上正次数多项式 $f(x)$ 在 F 上的分裂域. 若 $\mathrm{Gal}(E/F)$ 是可解群, 则 $f(x) = 0$ 在 F 上根式可解.

4.3.3*. 设 F 是任意特征的域, E/F 是有限可分扩张. 若 E/F 有根式扩张链, 则存在 E 的有限扩域 N, 使得 N/F 是有限正规扩张, 且 N/F 也有根式扩张链.

4.3.4*. 设域 F 的特征为零, E 是 F 上正次数多项式 $f(x)$ 在 F 上的分裂域. 若 $f(x)=0$ 在 F 上根式可解, 则 $\mathrm{Gal}(E/F)$ 是可解群.

第二部分　问题解答

第 1 章　群　　论

§1　集合与映射

知识要点:

集合的概念与运算: $\in$, $\notin$, $\subseteq$, $\supseteq$, $\subsetneqq$, $\supsetneqq$, $\not\subseteq$, $\not\supseteq$ 的意思; 并 $(A\bigcup B)$、交 $(A\bigcap B)$、差 $(A-B)$、卡氏积 $(A\times B)$、补 $(\bar{A})$.

映射、单射、满射、一一映射、逆映射、映射的合成.

二元运算.

集合上关系; 集合上的等价关系; 集合的划分; 集合上的等价关系和集合的划分之间的一一对应; 等价类与代表元系.

有限集与无限集、可数集与不可数集、集合的势.

偏序集; 链 (指偏序集的子集, 其中任意两个元均可比较); Zorn 引理: 如果偏序集 S 的任一链均有上界, 则 S 中必有极大元.

1.1.1. 设 B, A_i $(i\in I)$ 均是集合 Ω 的子集, 试证:

(1) $B\bigcap\left(\bigcup\limits_{i\in I}A_i\right)=\bigcup\limits_{i\in I}(B\bigcap A_i)$.

(2) $B\bigcup\left(\bigcap\limits_{i\in I}A_i\right)=\bigcap\limits_{i\in I}(B\bigcup A_i)$.

(3) $\overline{\bigcup\limits_{i\in I}A_i}=\bigcap\limits_{i\in I}\overline{A_i}$.

(4) $\overline{\bigcap\limits_{i\in I}A_i}=\bigcup\limits_{i\in I}\overline{A_i}$.

证　(1) 由定义 $x\in B\bigcap\left(\bigcup\limits_{i\in I}A_i\right)$ 当且仅当 $x\in B$ 且 x 属于某一 A_i; 当且仅当 x 属于某一 $B\bigcap A_i$; 当且仅当 $x\in\bigcup\limits_{i\in I}(B\bigcap A_i)$.

(2) 由定义 $x\in B\bigcup\left(\bigcap\limits_{i\in I}A_i\right)$ 当且仅当 x 属于 B, 或者 x 属于任一 A_i, $i\in I$:

当且仅当 x 属于任一 $B\bigcup A_i$, $i\in I$; 当且仅当 $x\in\bigcap\limits_{i\in I}(B\bigcup A_i)$.

(3) 由定义 $x\in\overline{\bigcup\limits_{i\in I}A_i}$ 当且仅当 $x\in\Omega$, $x\notin\bigcup\limits_{i\in I}A_i$; 当且仅当 $x\in\Omega$, x 不属于任何一个 A_i; 当且仅当 $x\in\bigcap\limits_{i\in I}\overline{A_i}$.

(4) 同理可证. ■

1.1.2. 设 $f:\ A\longrightarrow B$ 是集合的映射 (A, B 是非空集合), 试证:

(1) f 为单射 $\Longleftrightarrow$ 存在 $g:\ B\longrightarrow A$, 使得 $gf=1_A$.

(2) f 为满射 $\Longleftrightarrow$ 存在 $h:\ B\longrightarrow A$, 使得 $fh=1_B$.

证 (1) 若 f 是单射, 则可以定义 $g:B\longrightarrow A$ 如下:

$$g(b)=\begin{cases}a, & 若\ b=f(a),\\ a_0, & 否则,\end{cases}$$

其中 a_0 是 A 中某一固定元. 因 f 是单射, g 的定义是合理的, 则 $gf=1_A$. 反之, 设 $f(a_1)=f(a_2)$, a_1, $a_2\in A$. 则 $a_1=gf(a_1)=gf(a_2)=a_2$, 即 f 为单射.

(2) 同理可证. ■

1.1.3. 如果 $f:\ A\longrightarrow B$, $g:\ B\longrightarrow C$ 均是一一对应, 则 $gf:\ A\longrightarrow C$ 也是一一对应, 且 $(gf)^{-1}=f^{-1}g^{-1}$.

证 $(gf)(f^{-1}g^{-1})=g1_Bg^{-1}=1_C$, $(f^{-1}g^{-1})(gf)=f^{-1}1_Bf=1_A$. 故 gf 也是一一对应, 且 $(gf)^{-1}=f^{-1}g^{-1}$. ■

1.1.4. 设 A 是有限集, $P(A)$ 是 A 的全部子集 (包括空集) 所构成的集族. 试证 $|P(A)|=2^{|A|}$. 换言之, n 元集合共有 2^n 个不同的子集.

证 设 $|A|=n$, 则 A 共有 C_n^m 个 m 元子集, $0\leqslant m\leqslant n$. 故 $|P(A)|=\mathrm{C}_n^0+\mathrm{C}_n^1+\cdots+\mathrm{C}_n^{n-1}+\mathrm{C}_n^n=2^n$. ■

1.1.5. 设 $f:A\longrightarrow B$ 是集合的映射. 在集合 A 上如下定义一个关系: 对任意 a, $a'\in A$, $a\sim a'$ 当且仅当 $f(a)=f(a')$. 试证这样定义的关系是一个等价关系.

证 容易看出这种关系具有自反性 (即 $f(a)=f(a)$, $\forall\ a\in A$)、对称性 (即由 $f(a)=f(b)$ 可推出 $f(b)=f(a)$) 和传递性 (即由 $f(a)=f(b)$ 和 $f(b)=f(c)$ 可推出 $f(a)=f(c)$), 从而它是等价关系. ■

1.1.6. 设 A, B 是两个有限集合, 则

(1) A 到 B 的不同映射共有多少个?

(2) A 上不同的二元运算共有多少个?

(3) A 到 B 的单射共有多少个?

解 (1) 设 $|A|=n$, $|B|=m$, 则 A 到 B 有 m^n 个不同的映射.

(2) 设 $|A|=n$, 则 $|A\times A|=n^2$. 故由 (1) 知 $A\times A$ 到 A 有 n^{n^2} 个不同的映射. 即 A 上有 n^{n^2} 个不同的二元运算.

(3) 设 $|A|=n$, $|B|=m$. 若 $n>m$, 显然 A 到 B 没有单射; 若 $n\leqslant m$, 则 A 到 B 有 $\dfrac{m!}{(m-n)!}$ 个单射. ■

1.1.7*. 证明等价关系的三个条件是互相独立的, 即: 已知任意两个条件不能推出第三个条件.

证 例如, 实数集 $\mathbb{R}$ 中的关系 $\leqslant$ 满足自反性和传递性, 但不满足对称性.

实数集中关系 $\sim$ 满足自反性和对称性, 但不满足传递性, 其中 $a\sim b\Longleftrightarrow |a-b|\leqslant 1$.

在非负整数集 $\mathbb{N}_0$ 中定义关系 $\sim$, 其中 $a\sim b\Longleftrightarrow a$ 与 b 均为正数且有相同的奇偶性. 则易见 $\sim$ 满足对称性和传递性, 但不满足自反性: 因为没有 $0\sim 0$.

注 设关系 $\sim$ 满足: 对任一元 a, 均有元 b 使得 $a\sim b$. 则由 $\sim$ 的对称性和传递性可推出 $\sim$ 具有自反性. ■

1.1.8*. 设 V 是数域上的线性空间, 证明 V 有一组基.

证 V 的子集 L 称为线性无关的向量组, 如果 L 中任意有限个向量均是线性无关的.

令 S 是 V 中所有线性无关的向量组作成的集合, 则 S 对于集合的包含关系作成偏序集. 设 $T=\{L_i \mid i\in I\}$ 是 S 的一个链, 则 $L=\bigcup_{i\in I}L_i$ 也是线性无关的向量组. 事实上, 设 $\alpha_1,\cdots,\alpha_m$ 是 L 中任意有限个元, 则每个 α_i 属于某一 L_{j_i}. 因为 T 是链, 故存在 $i\in I$ 使得 $\alpha_1,\cdots,\alpha_m\in L_i$. 从而 $\alpha_1,\cdots,\alpha_m$ 是线性无关的.

于是 $L\in S$, L 是 T 的一个上界. 由 Zorn 引理知 S 有极大元 M. 不难验证 M 就是 V 的基: 即 M 是线性无关组, 且 V 中任一元均是 M 中有限个元的线性组合. ■

§2 群 的 概 念

知识要点:

群是带有一个二元运算的 (非空) 集合, 这个运算满足结合律, 具有单位元, 且任一元具有逆元.

群的简单性质: 单位元的唯一性、每个元的逆元的唯一性、左右消去律、穿脱原理 (指 $(ab)^{-1} = b^{-1}a^{-1}$).

群的简单例子: 数群、复数域 $\mathbb{C}$ 上的 n 次一般线性群 $GL(n,\mathbb{C})$; 复数域 $\mathbb{C}$ 上的 n 次特殊线性群 $SL(n,\mathbb{C})$; n 次正交群 $O(n,\mathbb{R})$; n 次酉群 $U(n,\mathbb{C})$; 整数环 $\mathbb{Z}$ 上的 n 次特殊线性群 $SL(n,\mathbb{Z})$ (特别地, 它对求逆封闭); 集合的变换群 (乘法是什么?); 剩余类加法群 (第一次遇到 "定义合理性" 问题).

群的稍进一步的性质 (单边定义; 除法定义; 有限半群成群的充要条件).

有限群的群表及其特性.

群同态与群同构及其意义.

群的自同构群.

1.2.1. 令 N 是所有 $n\times n$ 上三角非奇异复方阵的集合, P 是主对角线上的元都是 1 的上三角方阵的集合, 运算定义为矩阵的乘法. 试证 N 和 P 都是群.

证 方阵的乘法有结合律; n 阶单位阵是 N 的单位元; 两个 n 阶上三角非奇异复阵的积仍是 n 阶上三角非奇异复阵; 一个 n 阶上三角非奇异复阵的逆仍是 n 阶上三角非奇异复阵. 故依群的定义知 N 是群.

同理 P 是群. ■

1.2.2. 令 G 是实数对 (a,b), $a\neq 0$ 的集合, 在 G 上定义 $(a,b)(c,d) = (ac,\ ad+b)$. 试证 G 是群.

证 易证上述定义的乘法有结合律, $(1,0)$ 是其单位元, 任意元 $(a,b)\in G$ 有逆元 $(1/a, -b/a)$. 故由群的定义知 G 对于上述乘法成为群. ■

1.2.3. 令 Ω 是任意一个集合, G 是一个群, G^{Ω} 是 Ω 到 G 的所有映射的集合. 对任意两个映射 $f,g\in G^{\Omega}$, 定义乘积 fg 是这样的映射: 对任意 $a\in\Omega$, $(fg)(a) = f(a)\,g(a)$. 试证 G^{Ω} 是群.

证 易知上述乘法有结合律, $1\in G^{\Omega}$ 是其单位元, 其中 $1(a) = 1_G$, $\forall\, a\in\Omega$ (1_G 表示群 G 的单位元); 任一元 $f\in G^{\Omega}$ 有逆元 f^{-1}, 其中 $f^{-1}(a) := (f(a))^{-1}$, $\forall\, a\in\Omega$. 故 G^{Ω} 成为群. 这个群为 Abel 群当且仅当 G 是 Abel 群. ■

1.2.4. 令 G 是所有秩不大于 r 的 $n\times n$ 复方阵的集合, 试证在矩阵的乘法下 G 成半群.

证 注意到两个秩不大于 r 的 n 阶矩阵的积仍然是一个秩不大于 r 的 n 阶矩阵, 并且方阵的乘法满足结合律. 由定义即知 G 是半群. ■

1.2.5. 举出一个半群的例子, 它不是含幺半群; 再举出一个含幺半群的例子, 它不是群.

解 题 1.2.4 中的 G 是一个半群, 当 $r < n$ 时, 它不是一个含幺半群; 当 $r = n$ 时, 它是一个含幺半群, 但不是群.

又如, 整数集 $\mathbb{Z}$ 对于乘法成为一个含幺半群, 但不是群. ■

1.2.6*. (这可作为群的另一定义, 即群的单边定义) 设 G 是一个半群, 如果

(a) G 中含有左幺元 e, 即对任意 $a \in G$, $ea = a$;

(b) G 的每个元 a 有左逆 a^{-1}, 使得 $a^{-1} \cdot a = e$.

试证 G 是群.

证 用 $(a^{-1})^{-1}$ 表示 a^{-1} 的左逆元, 则

$$a \cdot a^{-1} = e(a \cdot a^{-1}) = (a^{-1})^{-1}a^{-1}aa^{-1} = (a^{-1})^{-1}ea^{-1} = (a^{-1})^{-1}a^{-1} = e.$$

这表明 a 的左逆元 a^{-1} 也满足 $a \cdot a^{-1} = e$. 而 $ae = a(a^{-1}a) = ea = a$, 这表明 e 是 G 的单位元, a^{-1} 是 a 的逆元, 故 G 是群. ■

1.2.7*. (这可作为群的另一定义: 即群的除法定义) 设 G 是半群, 若对任意 $a, b \in G$, 方程 $xa = b$ 和 $ay = b$ 在 G 内有解, 则 G 是群.

证 首先 G 非空, 故有 $a \in G$. 则 $xa = a$ 有解 e. 对于任一 $b \in G$, 有 $y \in G$ 使 $ay = b$. 于是

$$eb = eay = ay = b.$$

这表明 e 是 G 的左单位元. 而 $xb = e$ 有解则意味着 b 有左逆元. 因此由题 1.2.6 的结论可知 G 是群. ■

1.2.8*. (这可作为有限群的另一定义) 设 G 是一个有限半群, 如果在 G 内左右消去律均成立, 即由 $ax = ay$ 或 $xa = ya$ 可推出 $x = y$, 则 G 是群.

证 设 $G = \{a_1, \cdots, a_n\}$, 由消去律知

$$\{a_1a_i, \cdots, a_na_i\} = G = \{a_ia_1, \cdots, a_ia_n\},$$

$\forall a_i \in G$. 故存在 $e \in G$, 使得 $a_i = ea_i$.

于是对于任一 $a_j \in G$, 有 $a_k \in G$ 使得 $a_j = a_ia_k$. 从而

$$ea_j = ea_ia_k = a_ia_k = a_j.$$

这表明 e 是左单位元, 又因为 $e \in G = Ga_j$, 故 a_j 有左逆元. 由此即知 G 是群. ■

1.2.9. 设 G 是含幺半群, $a, b \in G$.

(1) 如果 a 有逆元 a^{-1}, 则 a^{-1} 也有逆元且 $(a^{-1})^{-1} = a$.

(2) 如果 a 和 b 都具有逆元, 则 ab 也有逆元, 且 $(ab)^{-1} = b^{-1}a^{-1}$.

证 由定义直接验证. ■

1.2.10. 设 $f: G \longrightarrow H$ 是群的同态, 则 $f(1_G) = 1_H$; 且对任意 $x \in G$ 有 $f(x^{-1}) = f(x)^{-1}$.

证 $f(1_G)f(1_G) = f(1_G \cdot 1_G) = f(1_G) = f(1_G)1_H$, 故由消去律知 $f(1_G) = 1_H$. 因为 $f(x^{-1})f(x) = f(x^{-1}x) = f(1_G) = 1_H$, 故 $f(x^{-1}) = f(x)^{-1}$. ■

1.2.11. 对任意 $a \in G$, $a \mapsto a^{-1}$ 是群 G 的自同构当且仅当 G 是 Abel 群.

证 将每一元变成其逆元是自同构 $\iff (ab)^{-1} = a^{-1}b^{-1}, \forall\, a, b \in G \iff ab = (a^{-1}b^{-1})^{-1} = ba, \forall\, a, b \in G \iff G$ 是 Abel 群. ■

1.2.12. 证明有理数加法群 $\mathbb{Q}$ 和非零有理数乘法群 $\mathbb{Q}^*$ 不同构.

证 若 $(\mathbb{Q}, +) \cong (\mathbb{Q}^*, \cdot)$, 则有群同构 f 和 $a \in \mathbb{Q}$ 使得 $f(a) = 2$, 从而 $2 = f(a) = f\left(\dfrac{a}{2} + \dfrac{a}{2}\right) = f\left(\dfrac{a}{2}\right)^2$, 即 $\sqrt{2}$ 是有理数, 矛盾. ■

1.2.13. 证明:

(1) 有理数加法群 $\mathbb{Q}$ 和正有理数乘法群 $\mathbb{Q}^+$ 不同构.

(2) 实数加法群 $\mathbb{R}$ 同构于正实数乘法群 $\mathbb{R}^+$.

证 (1) 题 1.2.12 的证明也适用于本题.

(2) 将每一实数 x 变到 e^x 就给出了实数加法群 $\mathbb{R}$ 到正实数乘法群 $\mathbb{R}^+$ 的同构映射. ■

1.2.14*. 在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解.

证 注意到若 $g^2 \neq 1$, 则 $(g^{-1})^2 \neq 1$ 且 $g \neq g^{-1}$. 因此 G 中满足 $x^2 \neq 1$ 的元 x 是成对出现的. 从而 G 中满足 $x^2 \neq 1$ 的元 x 有偶数个. 因此在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解. ■

1.2.15*. 令 G 是 n 阶有限群, S 是 G 的一个子集, $|S| > \dfrac{n}{2}$. 试证对任意 $g \in G$, 存在 $a, b \in S$ 使得 $g = ab$.

证 由消去律知, 对任一 $g \in G$, gS^{-1} 含有 $|S|$ 个元, 这里 S^{-1} 是 S 中元的所有逆元组成的集合. 因为 $|S| > \dfrac{|G|}{2}$, 故 $gS^{-1} \bigcap S \neq \varnothing$. 从而存在 $a, b \in S$, 使得 $gb^{-1} = a$, 即 $g = ab$. ■

1.2.16*. 求有理数加法群 $\mathbb{Q}$ 的自同构群 $\mathrm{Aut}(\mathbb{Q})$.

解 一方面, 对任一非零有理数 a, 将 x 变成 ax 是有理加法群 $\mathbb{Q}$ 的一个自同构. 记这个自同构为 f_a. 另一方面, 设 f 是有理数加群 $\mathbb{Q}$ 的任一自同构. 令

$f(1)=a$, 则 a 是非零有理数. 因为对任一正整数 n 和 m 有

$$f(n)=f(1+\cdots+1)=f(1)+\cdots+f(1)=nf(1)=na,$$
$$f(n)=f\left(\frac{n}{m}+\cdots+\frac{n}{m}\right)=f\left(\frac{n}{m}\right)+\cdots+f\left(\frac{n}{m}\right)=mf\left(\frac{n}{m}\right).$$

故得到

$$f\left(\frac{n}{m}\right)=\frac{1}{m}f(n)=\frac{n}{m}a.$$

由此推知 $f(x)=ax, \forall x\in\mathbb{Q}$, 即 $f=f_a$. 于是

$$\mathrm{Aut}(\mathbb{Q},+)=\{f_a|a\in\mathbb{Q},\ a\neq 0\}.$$

因为 $f_af_b=f_{ab}$, 故有群同构 $\mathrm{Aut}(\mathbb{Q},+)\cong(\mathbb{Q}^*,\cdot)$, 其中 $(\mathbb{Q}^*,\cdot)$ 是非零有理数的乘法群. ■

1.2.17*. b 是含幺半群 G 中的元 a 的逆元当且仅当成立 $aba=a$, $ab^2a=1$.

证 设 b 是 a 的逆元, 显然有 $aba=a$ 和 $ab^2a=1$. 反之, 若 $aba=a, ab^2a=1$, 则

$$ab=ab(ab^2a)=ab^2a=1,\quad ba=(ab^2a)ba=ab^2a=1.$$

即 b 是 a 的逆元. ■

1.2.18*. 令 G 是 n 阶有限群, $a_1,a_2,\cdots,a_n$ 是群 G 的任意 n 个元, 不一定两两不同. 试证存在整数 p 和 q, $1\leqslant p\leqslant q\leqslant n$, 使得 $a_pa_{p+1}\cdots a_q=1$.

证 令 $S=\{a_1,a_1a_2,\cdots,a_1a_2\cdots a_n\}$. 若 $1\in S$, 则结论已得证. 若 $1\notin S$, 因 $|G|=n$, 故 S 中至少有两个元是相等的. 设 $a_1\cdots a_i=a_1\cdots a_ia_{i+1}\cdots a_j$, 则 $a_{i+1}\cdots a_j=1$. ■

1.2.19*. 群 G 的自同构 α 称为没有不动点的自同构, 是指对 G 的任意元 $g\neq 1$ 有 $\alpha(g)\neq g$. 如果有限群 G 具有一个没有不动点的自同构 α 且 $\alpha^2=1$, 则 G 一定是奇数阶 Abel 群.

证 令 $H=\{g^{-1}\alpha(g)\,|\,g\in G\}$, 则 $H=G$. (事实上, 若 $g\neq h$, 则 $g^{-1}\alpha(g)\neq h^{-1}\alpha(h)$: 否则 hg^{-1} 是 α 的不动点, 从而 $g=h$. 矛盾!) 于是, 对任一 $a\in G, a=g^{-1}\alpha(g)$. 因 $\alpha^2=1$, 故 $a^{-1}=\alpha(g^{-1})g=\alpha(a)$. 从而 $\alpha(ab)=(ab)^{-1}=b^{-1}a^{-1}=\alpha(b)\alpha(a)=\alpha(ba)$. 故 $ba=ab, \forall a,\ b\in G$. 即 G 是 Abel 群. 因 $a^{-1}\neq a, \forall 1\neq a\in G$, 故 G 的阶为奇数. ■

1.2.20*. 设 a,b 是群 G 的两个元, 满足 $aba=ba^2b$, $a^3=1$, $b^{2n-1}=1$. 试证 $b=1$.

证 由题设条件得

$$ab^2a = aba^3ba = (aba)a^2ba = (ba^2b)a^2ba = ba^2(ba^2b)a = ba^2(aba)a = b^2a^2.$$

故 $ab^2 = b^2a$. 设 $ab^{2r} = b^{2r}a$, 则 $ab^{2(r+1)} = ab^{2r}b^2 = b^{2r}ab^2 = b^{2r}b^2a = b^{2(r+1)}a$. 因此对任一正整数 k 有 $ab^{2k} = b^{2k}a$. 特别地, 取 $k = n$ 得到 $ab^{2n} = b^{2n}a$. 因为 $b^{2n-1} = 1$, 所以 $b^{2n} = b$, 从而 $ab = ba$. 于是 $ba^2 = aba = ba^2b$. 故 $b = 1$. ■

§3 子群和陪集分解

知识要点:

子群的定义; 群 G 的子群 H 的单位元与 G 的单位元的一致性, 以及 H 中的元在 H 中的逆元与在 G 中的逆元的一致性.

子群的判定; 子群的简单例子: $SL(n,\mathbb{C}) < GL(n,\mathbb{C})$, $SO(n,\mathbb{R}) < O(n,\mathbb{R})$, $SU(n,\mathbb{C}) < U(n,\mathbb{C})$; 子群的交.

子群 H 和子群 K 的积 HK 成为子群的充要条件是 $HK = KH$.

群关于子群的左陪集划分和 Lagrange 定理 (特别地, 子群的阶能整除群的阶); 右陪集划分: 右陪集分解和左陪集分解的一种对应; 子群的指数的意义; 难点:(右) 陪集分解的一个完全代表元系; 应用举例:

(i) 元的阶及计算: 例如, $o(g^k) = \dfrac{o(g)}{(k, o(g))}$; 又例如, 若 $(o(g), o(h)) = 1$, $gh = hg$, 则 $o(gh) = o(g)o(h)$.

(ii) 两子群的积集的计数公式: $|AB| = \dfrac{|A||B|}{|A\bigcap B|}$, 其中 A, B 为群 G 的子群.

(iii) 中心、中心化子、共轭元的个数.

(iv) 类方程及其应用: p- 群有非平凡的中心; p 平方阶群是 Abel 群.

(v) 正规化子、共轭子群的个数.

1.3.1. 设 A 是群 G 的非空子集, 试证 A 是 G 的子群当且仅当对任意元 $a, b \in A, ab^{-1} \in A$ (这也相当于 $AA^{-1} = A$).

证 必要性显然, 只证充分性. 因 A 非空, 故有 $a \in A$, 从而 $1 = a \cdot a^{-1} \in A$. 设 $a, b \in A$, 则 $b^{-1} = 1 \cdot b^{-1} \in A$, 进而 $ab = a \cdot (b^{-1})^{-1} \in A$. 这就证明了 A 是 G 的子群. ■

1.3.2. 设群 G 中的元 g 的阶 $o(g) = mn$, $(m, n) = 1$. 则 $g = ab$, $o(a) = m$, $o(b) = n$, 且 a, b 均为 g 的幂.

证 因 $(m, n) = 1$, 故有整数 s, t 使得 $sm + tn = 1$, 而且 $(t, m) = 1 = (s, n)$.

令 $a=g^{tn}$, $b=g^{sm}$, 则 $g=ab$, 且

$$o(a)=o(g^{tn})=\frac{o(g)}{(tn,o(g))}=\frac{mn}{n(t,m)}=m.$$

同理 $o(b)=n$. ■

1.3.3. 设群 G 中两个元 g, h 可换, $o(g)=m$, $o(h)=n$. 记 (m,n), $[m,n]$ 分别是 m,n 的最大公因子和最小公倍数. 则

(1) $o(g^n h^m)=\dfrac{[m,n]}{(m,n)}$;

(2) G 中存在阶为 (m,n) 的元;

(3) G 中存在阶为 $[m,n]$ 的元.

证 (1) 因 $o(g^n)=\dfrac{m}{(m,n)}$, $o(h^m)=\dfrac{n}{(m,n)}$, $g^nh^m=h^mg^n$, $\left(\dfrac{m}{(m,n)},\dfrac{n}{(m,n)}\right)=1$, 故由已知结论知

$$o(g^nh^m)=\frac{m}{(m,n)}\frac{n}{(m,n)}=\frac{[m,n]}{(m,n)}.$$

(2) 设 $m=p_1^{m_1}\cdots p_t^{m_t}, n=p_1^{n_1}\cdots p_t^{n_t}$, 其中 $p_1,\cdots,p_t$ 是互不相同的素数, m_i,n_i 均为非负整数. 不妨设 $m_i\geqslant n_i, 1\leqslant i\leqslant l; m_i<n_i, l+1\leqslant i\leqslant t$. 令

$$a=p_1^{m_1}\cdots p_l^{m_l},\quad b=p_{l+1}^{n_{l+1}}\cdots p_t^{n_t}.$$

则 g^a 的阶为 $p_{l+1}^{m_{l+1}}\cdots p_t^{m_t}$, h^b 的阶为 $p_1^{n_1}\cdots p_l^{n_l}$. 这两个阶显然是互素的, 且 g^a 与 h^b 可换, 因此 g^ah^b 的阶为

$$(m,n)=p_1^{n_1}\cdots p_l^{n_l}p_{l+1}^{m_{l+1}}\cdots p_t^{m_t}.$$

(3) 类似可证. ■

1.3.4. 设 A 是群 G 的有限子集, 则 A 是 G 的子群当且仅当对任意元 a, $b\in A$, $ab\in A$.

证 必要性显然, 只证充分性. 此时 A 是有限半群且满足消去律, 从而 A 是群. ■

1.3.5. 设 A,B 分别是群 G 的两个子群, 试证 $A\bigcup B$ 是 G 的子群当且仅当 $A\leqslant B$ 或 $B\leqslant A$. 利用这个事实证明群 G 不能表示成两个真子群的并.

证 充分性显然, 只证必要性. 若 $A\not\subseteq B, B\not\subseteq A$, 则存在 $a\in A, a\notin B, b\in B, b\notin A$. 从而 $ab\notin A\bigcup B$, 这与 $A\bigcup B$ 是子群不合.

由此可知群 G 不能是其两个真子群之并 (否则 $G = H_1 \bigcup H_2$, 则由上述结论知 $G = H_1$ 或 $G = H_2$). ■

1.3.6. 设 A, B 是群 G 的两个子群, 试证 $AB \leqslant G$ 当且仅当 $AB = BA$.

证 若 $AB = BA$, 则易证 AB 对于乘法和求逆均封闭, 故 AB 是子群. 反之, 设 AB 是子群, 则对任意 $a \in A, b \in B$ 有

$$ba = (1 \cdot b)(a \cdot 1) \in (AB)(AB) \leqslant AB$$

即 $BA \leqslant AB$. 又有

$$ab = ((ab)^{-1})^{-1} \in (AB)^{-1} \leqslant B^{-1}A^{-1} = BA$$

即 $AB \leqslant BA$. 从而 $AB = BA$. ■

1.3.7. 设 A, B 是群 G 的两个子群且 $G = AB$. 如果子群 C 包含 A, 则 $C = A(B \bigcap C)$.

证 $\forall\, c \in C$, $c = ab$, $a \in A$, $b \in B$. 则 $b = a^{-1}c \in B \bigcap C$. 由此即知 $C = A(B \bigcap C)$. ■

1.3.8. 设 A 和 B 是有限群 G 的两个非空子集. 若 $|A| + |B| > |G|$, 则 $G = AB$.

证 $\forall g \in G$, $|Ag^{-1}| = |A|$. 因 $|A| + |B| > |G|$, 故 $A^{-1}g \bigcap B \neq \varnothing$, 于是有 $a \in A, b \in B$ 使得 $b = a^{-1}g$, 即 $g = ab$. 这表明 $G = AB$. ■

1.3.9. 设 A 和 B 均为群 G 的子群, 则

(1) $g(A \bigcap B) = gA \bigcap gB$, $\forall\, g \in G$.

(2) 若 A 和 B 均有有限的指数, 则 $A \bigcap B$ 也有有限的指数.

证 (1) $g(A \bigcap B) \subseteq gA$, $g(A \bigcap B) \subseteq gB$, 故 $g(A \bigcap B) \subseteq gA \bigcap gB$. 反之, $\forall\, x = gh \in gA \bigcap gB$, 则 $h \in A \bigcap B$, 从而 $x = gh \in g(A \bigcap B)$. 于是 $g(A \bigcap B) = gA \bigcap gB$, $\forall\, g \in G$.

(2) 本题 (1) 表明 $A \bigcap B$ 的任一左陪集是 A 的一个左陪集和 B 的一个左陪集之交. 若 A 和 B 均有有限个左陪集, 则 $A \bigcap B$ 也只有有限个左陪集. 由此即得证.

另证如下:

用 $\langle AB \rangle$ 表示 G 的由 AB 生成的子群. 则 $|\langle AB \rangle| \geqslant |AB| = \dfrac{|A||B|}{|A \bigcap B|}$. 两边

同乘 $\dfrac{|G|}{|A||B|}$ 得到

$$\frac{|G|}{|A\bigcap B|}\leqslant\frac{|G|}{|A|}\frac{|\langle AB\rangle|}{|B|}\leqslant\frac{|G|}{|A|}\frac{|G|}{|B|}<\infty. \qquad \blacksquare$$

1.3.10. 如果 R 是群 G 对于子群 A 的右陪集代表元系, 则 R^{-1} 是群 G 对于 A 的左陪集代表元系.

证 由题设知 $G=\bigcup\limits_{g\in R}Ag$, 并且满足 $Ag\bigcap Ah=\varnothing,\forall g\neq h,\ g,h\in R$. 需要验证 $G=\bigcup\limits_{x\in R^{-1}}xA$, 并且满足 $xA\bigcap yA=\varnothing,\ \forall\ x\neq y,\ x,y\in R^{-1}$. 这个验证是直接的.

事实上, $\forall\ z\in G$, 由题设 $z^{-1}\in Ag$, 对某一 $g\in R$, 于是 $z\in g^{-1}A^{-1}=g^{-1}A$. 即 $G=\bigcup\limits_{x\in R^{-1}}xA$. 若 $z\in xA\bigcap yA,\ x,y\in R^{-1}$, 即 $z=xa=yb,\ a,\ b\in A$, 从而

$$Ax^{-1}\bigcap Ay^{-1}=A(az^{-1})\bigcap A(bz^{-1})=Az^{-1}\neq\varnothing$$

其中 $x^{-1},\ y^{-1}\in R$. 从而由题设 $x^{-1}=y^{-1},\ x=y$. ■

1.3.11. 设 $A\leqslant G,\ B\leqslant G$. 如果存在 $a,\ b\in G$, 使得 $Aa=Bb$, 则 $A=B$.

证 因 $A=Bba^{-1}$, 故 $ba^{-1}\in A$, 但 A 是子群, 故 $(ba^{-1})^{-1}=ab^{-1}\in A$. 于是 $A=Aab^{-1}=Bbb^{-1}=B$. ■

1.3.12. 设 $n>2$, 则有限群 G 中有偶数个阶为 n 的元.

证 若 G 无 n 阶元, 则结论成立. 若 G 有 n 阶元 g, 则 g^{-1} 也是 n 阶元且 $g\neq g^{-1}$. 于是 $\{g,\ g^{-1}\}$ 是 n 阶元的一个集合.

一般地, 若 A 是 G 中 n 阶元的一个集合且 $A=A^{-1},\ o(x)=n,\ x\notin A$, 则 $o(x^{-1})=n$ 且 $x^{-1}\notin A$. 由此可见 G 中 n 阶元有偶数个. ■

1.3.13. 设 $a,\ b$ 是群 G 的任意两个元, 试证 a 和 a^{-1}, ab 和 ba 有相同的阶.

证 易证 a 和 a^{-1} 有相同的阶. 因 $ba=a^{-1}(ab)a$, 即 ba 和 ab 共轭, 故 ba 和 ab 的阶相同. ■

1.3.14*. 设 $A\leqslant G$, 试证 $C_GC_GC_G(A)=C_G(A)$.

证 令 $B=C_GC_G(A)$, 要证 $C_G(B)=C_G(A)$.

设 $x\in C_G(A)$. 对于任一 $y\in B=C_GC_G(A)$, 由定义知 y 与 x 可换, 即 x 和 y 可换, 即 $x\in C_G(B)$. 故 $C_G(A)\leqslant C_G(B)$.

反之, 设 $y \in C_G(B)$, 即 y 与 B 中任一元可换. 因为 $C_G(A)$ 中任一元与 A 中任一元可换, 故 A 中任一元与 $C_G(A)$ 中的元可换. 由定义

$$A \leqslant C_G C_G(A) = B.$$

从而 y 与 A 中任一元可换, 即 $y \in C_G(A)$. 故 $C_G(B) \leqslant C_G(A)$. 从而 $C_G(B) = C_G(A)$. ■

1.3.15*. 试证有限群 G 的一个真子群的全部共轭子群之并不能覆盖整个群 G. 结论对无限群是否成立?

证　设 H 是 G 的真子群, 则 H 共有 $[G : N_G(H)]$ 个共轭子群. 令 Σ 是 H 的所有共轭子群之并, 则

$$|\Sigma| \leqslant (|H| - 1)[G : N_G(H)] + 1 = \frac{|G|}{|N_G(H)|} \cdot |H| - [G : N_G(H)] + 1.$$

若 H 是正规子群, 则 $N_G(H) = G$, 于是

$$|\Sigma| \leqslant |H| - 1 + 1 = |H| < |G|.$$

若 H 不是正规子群, 则 $N_G(H) \neq G$, 于是 $[G : N_G(H)] > 1$,

$$|\Sigma| \leqslant \frac{|G|}{|H|} \cdot |H| - [G : N_G(H)] + 1 < |G| - 1 + 1 = |G|.$$

综合以上, $|\Sigma| < |G|$, 即 H 的全部共轭子群之并不能覆盖 G.

这一结论对无限群不再成立. 例如, 令 $G = GL(n, \mathbb{C})$, H 是 n 阶上三角可逆复矩阵作成的真子群. 由 Jordan 标准型知任一 n 阶可逆阵 A 相似于某一 H 中的元, 这表明 G 是 H 的所有共轭子群之并. ■

1.3.16*. 设 H 和 K 分别是有限群 G 的两个子群, 试证:

$$|HgK| = |H|[K : K \bigcap g^{-1}Hg] = |K|[H : H \bigcap gKg^{-1}].$$

证　集合 HgK 称为 G 的一个双陪集. 为了计算 $|HgK|$, 将 HgK 分解为 G 关于 H 的右陪集的无交之并

$$HgK = Hgk_1 \bigcup \cdots \bigcup Hgk_t$$

因此 $|HgK| = |H| \cdot t$. 注意到集合 $\{k_1, \cdots, k_t\}$ 是 K 关于子群 $K \bigcap g^{-1}Hg$ 的右陪集的一个代表元系, 即有下述无交并

$$K = \bigcup_{1 \leqslant i \leqslant t} (K \bigcap g^{-1}Hg)k_i.$$

于是 $t=[K:K\bigcap g^{-1}Hg]$. 从而

$$\begin{aligned}|HgK|&=|H|\cdot[K:K\bigcap g^{-1}Hg]\\&=\frac{|H||K|}{|K\bigcap g^{-1}Hg|}=|K|\frac{|H|}{|H\bigcap gKg^{-1}|}=|K|[H:H\bigcap gKg^{-1}].\end{aligned}$$

注 在 G 上定义关系 $\sim$: $x\sim y \iff x\in HyK$, 容易验证 $\sim$ 是等价关系. 由此可知 G 可以写成无交之并 $G=\bigcup\limits_{g_i\in R}Hg_iK$, 这里 R 称为 G 关于 (H,K)- 双陪集的一个代表元系. ■

1.3.17*. 设 A 是群 G 的具有有限指数的子群, 试证: 存在 G 的一组元 $g_1,g_2,\cdots,g_m$, 它们既可以作为 A 在 G 中的右陪集代表元系, 又可以作为 A 在 G 中的左陪集代表元系.

证 由题 1.3.16 的注记, 可将 G 写成双陪集的无交并: $G=\bigcup\limits_{g\in R}AgA$. 由题 1.3.16 知每个双陪集 AgA 既是 $[A:A\bigcap gAg^{-1}]$ 个互不相交右陪集之并, 也是 $[A:A\bigcap gAg^{-1}]$ 个互不相交左陪集之并. 记 $t=[A:A\bigcap gAg^{-1}]$, 则有无交并

$$AgA=\bigcup_{1\leqslant i\leqslant t}Aga_i=\bigcup_{1\leqslant i\leqslant t}b_igA,$$

其中 a_i, $b_i\in A$. 于是 $A=Ab_i=a_iA$, 故有无交并

$$AgA=\bigcup_{1\leqslant i\leqslant t}Ab_iga_i,\quad AgA=\bigcup_{1\leqslant i\leqslant t}b_iga_iA.$$

记 $b_i=b_i(g)$, $a_i=a_i(g)$, $t=t(g)$, 于是

$$\bigcup_{g\in R}\{\ b_i(g)ga_i(g)\ \mid\ 1\leqslant i\leqslant t(g)\}$$

既是 G 关于 A 的右陪集的一个代表元系, 也是 G 关于 A 的左陪集的一个代表元系, 这里 R 是 G 关于 (A,A)- 双陪集的一个代表元系. ■

1.3.18*. 令 $G=GL(n,\mathbb{C})$, P 是主对角线上的元均为 1 的 $n\times n$ 上三角方阵全体形成的 G 的子群. 确定 $N_G(P),C_G(P)$ 和 P 的中心 $Z(P)$.

解 由矩阵的乘法直接计算可知与任一 n 阶主对角线为 1 的上三角矩阵可换的矩阵必为上三角矩阵, 且形如

$$J_n(\lambda,\mu)=\begin{pmatrix}\lambda&0&\cdots&0&\mu\\&\lambda&\cdots&0&0\\&&\ddots&\vdots&\vdots\\&&&\lambda&0\\&&&&\lambda\end{pmatrix},$$

其中 $\mu \in \mathbb{C}$. 要看出这一点, 只要取主对角线为 1 且 $(i,i+1)$ 处为 1, 其余全为 0 的上三角矩阵即可, $i=1,\cdots,n-1$. 因此

$$C_G(P)=\{J_n(\lambda,\mu)\,|\,\lambda,\mu\in\mathbb{C},\lambda\neq 0\}.$$

由此即知 $Z(P)=\{J_n(1,\mu)\mid \mu\in\mathbb{C}\}$.

下面求

$$\begin{aligned}N_G(P):&=\{A\in GL(n,\mathbb{C})\,|\,AP=PA\}\\&=\{A\in GL(n,\mathbb{C})\,|\,AJA^{-1}\subseteq P,\ A^{-1}JA\subseteq P,\ \forall\ J\in P\}.\end{aligned}$$

首先, 所有 n 阶上三角可逆矩阵均在 $N_G(P)$ 中. 我们断言: $N_G(P)$ 恰是所有 n 阶上三角可逆矩阵作成的群.

设 A 是 n 阶可逆矩阵且 A 不是上三角的. 设 a_{ij} 是 A 中主对角线以下的非零元且 i 最大, 即

$$a_{ij}\neq 0, i>j;\ 且若\ a_{st}\neq 0, s>t, 则\ i\geqslant s.$$

令 J 是主对角线全为 1 且 $(j,j+1)$ 处为 1, 其余全为 0 的矩阵. 则 AJ 是将 A 的第 j 列加到第 $j+1$ 列后得到的矩阵, 从而 AJ 不是上三角的.

下证 $A\notin N_G(P)$. 否则存在 $B\in P$ 使得 $AJ=BA$, 注意到 AJ 的第 $(i,j+1)$ 处元是

$$a_{i,j}+a_{i,j+1}.$$

但 BA 是对 A 施行一系列初等行变换得到的, 这些行变换是将大数行的若干倍加到小数行. 由 A 的选取知 BA 的 $(i,j+1)$ 处元与 A 的 $(i,j+1)$ 处元相同, 均为 $a_{i,j+1}$, 从而 $AJ\neq BA$, 矛盾. 所以 $A\notin N_G(P)$. 即 $N_G(P)$ 恰是所有 n 阶上三角可逆矩阵作成的群. ■

1.3.19*. 设 G 是有限 Abel 群, 试证 g 对应到 g^k 是 G 的一个自同构当且仅当 k 和 $|G|$ 互素.

证　令 $o(g)$ 是 g 的阶.

充分性: 设 $|G|$ 与 k 互素, 令

$$\alpha:\ G\longrightarrow G,\ \alpha(g)=g^k, \forall g\in G.$$

因 G 是 Abel 群, 故 α 是群同态. 设 $\alpha(g)=\alpha(h)$, 即 $(h^{-1}g)^k=1$. 又因为 $h^{-1}g$ 的阶是 $|G|$ 的因子, 由题设知 k 和 $h^{-1}g$ 的阶互素. 由此即可推出 $h=g$, 即 α 是单射. 设 $l|G|+mk=1$, 则对任一 $g\in G$ 有

$$g=g^{l|G|+mk}=(g^m)^k.$$

这表明 α 是满射, 即 α 是群 G 的自同构.

必要性: 设 $\alpha: G \longrightarrow G$, $\alpha(g) = g^k, \forall g \in G$ 是群自同构. 则对任一 $g \in G$, g 与 $g^k = \alpha(g)$ 的阶相同. 另一方面, 根据已知的公式

$$o(g^k) = \frac{o(g)}{(k, o(g))},$$

即知 k 和 $o(g)$ 互素, 对 $\forall g \in G$ 成立.

对 $|G|$ 用数学归纳法证明 k 与 $|G|$ 互素. 若 $|G| = o(g)$, 则已证. 设 $o(g) < |G|, \forall g \in G$. 令 $1 \neq a \in G, o(a) = n < |G|$. 考虑 G 的商群 $\overline{G} = G/\langle a \rangle$, 则上述 α 诱导出 $\overline{G}$ 的满自同态. 下证 α 作为 $\overline{G}$ 的自同态也是单射. 事实上, 若 $\alpha(\overline{g}) = \alpha(\overline{h})$, 即 $(h^{-1}g)^k \in \langle a \rangle$, 则

$$(h^{-1}g)^{kn} = 1.$$

这推出 $(h^{-1}g)^n = 1$. 设 $ln + mk = 1$, 于是

$$h^{-1}g = (h^{-1}g)^{mk} \in \langle a \rangle.$$

即 $\overline{h} = \overline{g}$, 故 α 是单射. 因此, 由数学归纳法知 k 和 $|G|/n$ 互素. 而已知 k 与 n 互素, 从而 k 与 $|G|$ 互素.

注 如果应用 Sylow 定理, 则只要证 k 与任一元的阶互素即可 (从而上述证明的最后一段可以删去): 对 $|G|$ 的任一素因子 p, 存在 p 阶元 g, 故 k 与 p 互素, 从而 k 与 $|G|$ 互素. ∎

1.3.20*. 设 G 是奇数阶有限群, $\alpha \in \mathrm{Aut}(G)$ 且 $\alpha^2 = 1$. 令

$$G_1 = \{g \in G \mid \alpha(g) = g\}, \quad G_{-1} = \{g \in G \mid \alpha(g) = g^{-1}\}.$$

试证: $G = G_1 G_{-1}$ 且 $G_1 \bigcap G_{-1} = 1$.

证 由题设知 $(2, |G|) = 1$, 因此 G 中任一元均可写成某一元的平方的形式. 对任一 $g \in G$, 设 $g^{-1}\alpha(g) = x^2$. 因

$$\alpha(x)^2 = \alpha(g^{-1}\alpha(g)) = \alpha(g)^{-1}g = (g^{-1}\alpha(g))^{-1} = x^{-2},$$

而 x 和 $\alpha(x)$ 的阶相同且为奇数, 由此容易推出 $\alpha(x) = x^{-1}$, 即 $x \in G_{-1}$. 又因为

$$\alpha(gx) = \alpha(g)\alpha(x) = \alpha(g)x^{-1} = gx,$$

即 $gx \in G_1$, 故

$$g = (gx)x^{-1} \in G_1 G_{-1},$$

即 $G = G_1G_{-1}$.

若 $g \in G_1 \bigcap G_{-1}$, 则 $g^2 = 1$. 但 $|G|$ 是奇数, 故 $g = 1$, 即 $G_1 \bigcap G_{-1} = 1$. ■

1.3.21*. 设群 G 的元 a_1, a_2, b_1, b_2 满足

$$a_1b_1 = a_2b_2 = b_1a_1 = b_2a_2, \quad a_1^m = a_2^m = b_1^n = b_2^n = 1,$$

其中 m 和 n 是互素的正整数. 则 $a_1 = a_2$, $b_1 = b_2$.

证　设 k, l 是整数使得 $km + ln = 1$. 由 $a_1b_1 = a_2b_2$ 知

$$(a_1b_1)^{km} = (a_2b_2)^{km}.$$

因 $a_1b_1 = b_1a_1$, $a_2b_2 = b_2a_2$, $a_1^m = 1 = a_2^m$, 故

$$(a_1b_1)^{km} = a_1^{km}b_1^{km} = b_1^{km}, \quad (a_2b_2)^{km} = a_2^{km}b_2^{km} = b_2^{km}.$$

从而有 $b_1^{km} = b_2^{km}$. 而 $b_1^{ln} = b_2^{ln} = 1$, 故 $b_1 = b_1^{km+ln} = b_2^{km+ln} = b_2$.

同理可证 $a_1 = a_2$. ■

§4　循　环　群

知识要点:

固定阶循环群在同构意义下的唯一性: 无限循环群同构于整数加法群; n 阶循环群同构于模 n 的剩余类加法群 $\mathbb{Z}_n$.

循环群的全部子群; 特别地, 无限循环群的子群是无限循环群;n 阶循环群的子群是 m 阶循环群, 其中 $m \mid n$; 有限循环群的固定阶子群在集合意义下的唯一性.

无限循环群 $\langle a\rangle$ 的生成元只有 a 和 a^{-1}; n 阶循环群 $\langle a\rangle$ 的生成元为 a^k, $(k,n) = 1$, $1 \leqslant k < n$.

无限循环群 $\langle a\rangle$ 的自同构群同构于 $\mathbb{Z}_2$; n 阶循环群 $\langle a\rangle$ 的自同构群同构于 $U(\mathbb{Z}_n)$ (即 $\mathbb{Z}_n$ 中乘法可逆元作成乘法群).

1.4.1. 证明 Euler 定理: 若 n 是正整数, a 是与 n 互素的整数, 则 $a^{\varphi(n)} \equiv 1 \pmod n$, 其中 $\varphi(n)$ 是 Euler 函数, 即 $\varphi(n)$ 是与 n 互素的不超过 n 的正整数的个数.

特别地, 若 p 是素数, 则得到 Fermat 小定理: $a^p \equiv a \pmod p$, $\forall\, a \in \mathbb{Z}$.

证　$\mathbb{Z}_n$ 中乘法可逆的元作成 $\varphi(n)$ 阶群, 记为 $\mathbb{Z}_n^*$. 因 $(a,n) = 1$, 故 $\overline{a} \in \mathbb{Z}_n^*$. 于是在群 $\mathbb{Z}_n^*$ 中有 $(\overline{a})^{\varphi(n)} = \overline{1}$, 即 $a^{\varphi(n)} \equiv 1 \pmod n$.

若 p 是素数, 则 $\varphi(p) = p - 1$. 因此, 若 $p \nmid a$, 则 $a^{p-1} \equiv 1 \pmod p$, 从而 $a^p \equiv a \pmod p$. 此式对 $p \mid a$ 也是对的. ■

1.4.2. 设 n 是正整数, 试证: 满足方程 $x^n = 1$ 的复数的集合 G 在通常乘法下是一个 n 阶循环群.

证 $G = \left\{\cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n} \mid k = 0, 1, \cdots, n-1\right\} = \left\langle \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n} \right\rangle$. ■

1.4.3. 群 G 没有非平凡子群的充分必要条件是 $G = \{1\}$ 或是素数阶循环群.

证 充分性显然, 只证必要性. 设 $G \neq \{1\}$. 因为 G 无非平凡子群, 故 $G = \langle g \rangle, \forall\, 1 \neq g \in G$. 同样的原因 g 的阶只能是素数. ■

1.4.4. (1) 设 a 和 b 是群 G 的元, 阶数分别是 n 和 m, $(n, m) = 1$ 且 $ab = ba$. 求 $|\langle ab \rangle|$.

(2) 设群 G 中元 g 的阶 $o(g)$ 与正整数 n 互素, 在 $\langle g \rangle$ 中求解方程 $x^n = g$.

解 (1) 因为 $ab = ba$ 且 a 的阶与 b 的阶互素, 故 ab 的阶恰为 mn. 因此 $\langle ab \rangle$ 的阶是 mn.

(2) 设 $so(g) + tn = 1$, $s, t \in \mathbb{Z}$. 于是 $g = g^{tn}$, 故 $x = g^t \in \langle g \rangle$ 是方程 $x^n = g$ 的解.

设 $x = g^m$, g^t $(0 \leqslant t \leqslant m \leqslant o(g) - 1)$ 均是 $x^n = g$ 的解. 则由 $g^{mn} = g$ 知 $mn \equiv 1$, $tn \equiv 1 \pmod{o(g)}$. 从而 $o(g) \mid (m-t)n$, $o(g) \mid (m-t)$, 于是 $m = t$. 即在 $\langle g \rangle$ 中方程 $x^n = g$ 有唯一的解. ■

1.4.5. 真子群 M 称为群 G 的极大子群, 如果不存在 G 的子群 B, 使得 $M < B < G$. 确定无限循环群的全部极大子群.

解 无限循环群 $\mathbb{Z}$ 的任一子群形如 $n\mathbb{Z}$, 这里 n 是非负整数. 它是极大子群当且仅当 n 为素数. ■

1.4.6*. 如果有限群 G 有唯一的极大子群, 则 G 是素数幂阶循环群.

证 首先回顾极大子群的定义: 群 G 的子群 H 称为 G 的极大子群, 如果 $H \neq G$, 并且包含 H 的子群只有 G 和 H 本身.

设 H 是 G 的唯一极大子群. 因为 G 是有限群, 故 G 的任一真子群必含于 G 的某一极大子群之中. 因为 H 是 G 的唯一极大子群, 故 H 也是 G 的最大子群, 即 H 包含 G 的任一真子群. 取 $g \notin H$, $g \in G$, 则 $G = \langle g \rangle$ (否则得到矛盾 $\langle g \rangle \subseteq H$).

若 g 的阶含有两个不同的素因子 p 和 q, 则 $\langle g^p \rangle$ 和 $\langle g^q \rangle$ 均是 G 的真子群. 从而 $\langle g^p \rangle$, $\langle g^q \rangle \subseteq H$. 因为 $(p, q) = 1$, 所以存在整数 l, m 使得 $lp + mq = 1$. 故 $g = g^{lp+mq} \in H$, 矛盾! ■

1.4.7. 举一个无限群的例子, 它的任意阶数不为 1 的子群都具有有限指数.

解 设 H 是无限循环群 $\mathbb{Z}$ 的阶数不为 1 的子群, 则 $H=n\mathbb{Z}$, 它的指数为 n, 这里 n 是正整数. ■

1.4.8. 设 p 是一个素数, $G=\{x\in\mathbb{C}\mid$ 存在正整数 n 使得 $x^{p^n}=1\}$, 则 G 对于复数的乘法作成群. 试证 G 的任意真子群都是有限阶的循环群.

证 设 H 是 G 的真子群, 故存在 $g\in G$, $g\notin H$. 设 g 的阶为 p^n, 则 H 中任一元的阶为 p^m, $m<n$. 否则, H 中有元 h 的阶为 p^m, $m\geqslant n$, 则 h 是 $x^{p^m}-1=0$ 的解集作成的 p^m 阶循环群 L 的生成元. 因为 $m\geqslant n$, 故 $g\in L\subseteq H$, 矛盾! 设 h 是 H 中阶最大的元, 则 $H=\langle h\rangle$. ■

1.4.9. 若群 G 只有有限多个子群, 则 G 是有限群.

证 由假设 G 中元的阶均为有限, 否则, G 有同构于 $\mathbb{Z}$ 的子群, 而 $\mathbb{Z}$ 有无限个子群 $n\mathbb{Z}$.

由假设 G 只有有限多个循环子群. 另一方面, $G=\bigcup\limits_{a\in G}\langle a\rangle$. 所以存在有限个元 $a_1,\cdots,a_n$, 使得 $G=\bigcup\limits_{1\leqslant i\leqslant n}\langle a_i\rangle$; 而每个 $\langle a_i\rangle$ 均为有限群, 从而 G 是有限群. ■

1.4.10*. 有理数加法群 $\mathbb{Q}$ 不是循环群, 但它的任意有限生成的子群都是循环群.

证 设 $\dfrac{m}{n}\in\mathbb{Q}$. 取素数 p, p 不是 n 的因子, 则 $\dfrac{1}{p}\notin\left\langle\dfrac{m}{n}\right\rangle$. 这表明 $\mathbb{Q}$ 不是循环群.

欲证 $\mathbb{Q}$ 的有限生成子群是循环群, 由归纳法只要证由两个元生成的子群是循环群即可. 设 $H=\left\langle\dfrac{m}{n},\dfrac{t}{s}\right\rangle$, 令 $d=(ms,nt)$. 则 $\dfrac{d}{ns}\in\left\langle\dfrac{m}{n},\dfrac{t}{s}\right\rangle$, 且 $\dfrac{m}{n}\in\left\langle\dfrac{d}{ns}\right\rangle$, $\dfrac{t}{s}\in\left\langle\dfrac{d}{ns}\right\rangle$. 故 $H=\left\langle\dfrac{d}{ns}\right\rangle$. ■

1.4.11*. 在 n 阶循环群 G 中, 对 n 的每个正因子 m, 阶为 m 的元恰好有 $\varphi(m)$ 个, 其中 $\varphi(m)$ 是与 m 互素且不超过 m 的正整数的个数. 由此证明等式 $\sum\limits_{m|n}\varphi(m)=n$.

证 设 $G=\langle a\rangle$, m 是 n 的一个正因子, 则 G 中阶为 m 的元恰好有 $\varphi(m)$ 个. (事实上, 若 $o(a^k)=m$, 则

$$\frac{n}{(n,k)}=m,\quad (n,k)=\frac{n}{m}.$$

于是 $k=q\dfrac{n}{m}$, q 为正整数. 从而 $(n,k)=\left(n,q\dfrac{n}{m}\right)=\dfrac{n}{m}(m,q)$. 于是 $(m,q)=1$,

$1 \leqslant q \leqslant m$. 这样的 q 恰有 $\varphi(m)$ 个.)

现在来数 G 中元的个数. 因为 G 中任一元的阶均是 n 的正因子, 故 $n = |G| = \sum\limits_{m|n} \varphi(m)$. ■

1.4.12*. 设 G 是一个 n 阶有限群, 若对 n 的每一个因子 m, G 中至多只有一个 m 阶子群, 则 G 是循环群.

证 设 G 中元的全部阶为 $d_1, \cdots, d_t$. 我们断言: G 中阶为 d_i 的元恰有 $\varphi(d_i)$ 个, $i = 1, 2, \cdots, t$. (事实上, 设 $a, x \in G$, 并设 $o(a) = d_i$. 若 $o(x) = d_i$, 则 $\langle a \rangle$ 与 $\langle x \rangle$ 均是 d_i 阶子群. 由题设知:$\langle a \rangle = \langle x \rangle$, 从而 $x = a^k$, $(k, d_i) = 1$, $1 \leqslant k < d_i$, 这样的 k 恰有 $\varphi(d_i)$ 个, 从而这样的元 x 恰有 $\varphi(d_i)$ 个.)

由题 1.4.11 得到

$$\sum_{i=1}^{t} \varphi(d_i) = n = \sum_{m|n} \varphi(m) \qquad (*)$$

注意到 $\{d_1, \cdots, d_t\} \subseteq \{m \mid m \text{ 是 } n \text{ 的正因子 }\}$, $\varphi(m)$ 是正整数, 故 $(*)$ 式意味着这两个集合必相等, 从而存在 i 使 $d_i = n$. 即 G 是循环群. ■

1.4.13*. 群 G 是循环群当且仅当 G 的任一子群形如 $G^m = \{g^m | \ g \in G\}$, 其中 m 是非负整数.

证 必要性易证, 只证充分性. 设 G 的任一子群形如 $G^m = \{g^m | \ g \in G\}$, 其中 m 是非负整数.

首先设 G 有无限阶元 a. 由题设 $\langle a \rangle = G^m$, $m > 0$. 于是有 $b \in G$ 使得 $a = b^m$. 由题设 $\langle b \rangle = G^n$, $n > 0$. 于是有 $c \in G$ 使得 $b = c^n$. 因 $c^m \in G^m = \langle a \rangle$, 故有

$$c^m = a^i = b^{mi} = c^{nmi}.$$

显然 c 是无限阶元, 于是 $m = nmi$. 从而 $1 = ni$, $n = 1$. 于是 $G = G^n = \langle b \rangle$ 是循环群.

下设 G 中任一元的阶均有限. 容易知道 G 有素数 p 阶元 g, 则 $\langle g \rangle = G^n$. 设 x 是 G 中任一元, 则 $x^n \in \langle g \rangle$, 故 $x^{pn} = 1$, 从而 $o(x) \mid pn$. 因此 G 中元的阶的集合是有界集. 设 $\{p_1, \cdots, p_m\}$ 是 G 中元的阶的素因子的集合.

设 $H \leqslant G$, 则 $H = G^t$. 因此 $xHx^{-1} = xG^tx^{-1} = G^t = H$, 即 G 的任一子群均为正规子群.

设 g 是素数 p 阶元, 则 g 是中心元. 事实上, $\forall\ x \in G$, $xgx^{-1} = g^i$. 不妨设 $2 \leqslant i \leqslant p-1$, 又 $g^{-1}xg = x^j$. 于是

$$gx^j = xg = g^ix,$$

从而 $g^{i-1}=x^{j-1}$. 因 $(i-1,p)=1$, 故 g 由 g^{i-1} 生成, 从而 g 是 x 的幂, 于是 g 与 x 可换.

现在对每个 p_i, 容易知道可取到 p_i 阶元 g_i. 因此由上所述, $g=g_1\cdots g_m$ 是阶为 $p_1\cdots p_m$ 的元. 于是总可取到 G 中元 h, h 的阶有因子 $p_1\cdots p_m$, 且 h 的阶是具有这种性质的元的阶中最大的一个. 则 $\langle h\rangle=G^k$. 于是有 $h=a^k$, 则

$$o(h)=o(a^k)=\frac{o(a)}{(k,o(a))}.$$

则 a 的阶也有因子 $p_1\cdots p_m$, 故由 h 的取法知 $o(a)\leqslant o(h)\leqslant o(a)$. 从而 $o(h)=o(a)$ 且 $(k,o(a))=1$, 从而 $(k,p_1\cdots p_m)=1$.

设 x 是 G 中任一元, 则 $(k,o(x))=1$ (因为 $o(x)$ 的素因子属于 $\{p_1,\cdots,p_m\}$). 于是存在整数 l,l', 使得 $1=lk+l'o(x)$, 从而

$$x=(x^l)^k\in G^k=\langle h\rangle,$$

即 $G=\langle h\rangle$. ■

§5 正规子群和商群

知识要点:

正规子群的定义和等价说法; 正规子群的例子; 商群的构造与意义; 群同态基本定理的表述、意义和证明; 群同态基本定理的应用: 子群对应定理和两个同构定理; 应用举例: 如群 G 的内自同构群同构于 $G/Z(G)$, 其中 $Z(G)$ 是 G 的中心.

1.5.1. 令 G 是实数对 (a,b), $a\neq 0$ 带有乘法 $(a,b)(c,d)=(ac,ad+b)$ 的群. 试证: $K=\{(1,b)|\ b\in\mathbb{R}\}$ 是 G 的正规子群且 $G/K\cong\mathbb{R}^*$, 这里 $\mathbb{R}^*$ 是非零实数的乘法群.

证 直接验证 $K\lhd G$. 考虑群同态 $\pi:\ G\longrightarrow\mathbb{R}^*$, $\pi(a,b)=a$. 这显然是满同态且 $\operatorname{Ker}\pi=K$. 故由群同态的基本定理知 $G/K\cong\mathbb{R}^*$. ■

1.5.2. 设 G 是群, $N<M<G$.

(1) 如果 $N\lhd G$, 则 $N\lhd M$.

(2) 如果 $N\lhd M$, $M\lhd G$, N 是否一定是 G 的正规子群?

证 (1) 直接按照定义可证.

(2) 正规子群不具有传递性. 例如, $\mathbb{Z}_2\lhd K_4\lhd S_4$, 其中 K_4 是 Klein 四元群. 但 $\mathbb{Z}_2$ 不是 S_4 的正规子群. ■

1.5.3. 试证:

(1) 群 G 的中心 $Z(G)$ 是 G 的正规子群.

(2) 群 G 的指数为 2 的子群 N 一定是 G 的正规子群.

证 (1) 直接由定义可证.

(2) 因 $[G:N]=2$, 故 $G=N\bigcup gN=N\bigcup Ng$, $\forall g\notin N$. 于是 $gN=Ng$, $\forall g\in G$. 即 $N\lhd G$. ■

1.5.4. (1) 设 $N\lhd G$, M 是 G 的子群且 $N\leqslant M$. 则 $N_G(M)/N=N_{\overline{G}}(\overline{M})$, 这里 $\overline{G}=G/N$, $\overline{M}=M/N$.

(2) 设 $f:\ G\longrightarrow H$ 是群同态, $M\leqslant G$. 试证 $f^{-1}(f(M))=KM$, 这里 $K=\operatorname{Ker} f$.

(3) 设 $f:G\longrightarrow H$ 是群同态. 若 g 是 G 的一个有限阶元, 则 $f(g)$ 的阶整除 g 的阶.

证 (1) 注意到 $N_{\overline{G}}(\overline{M})$ 形如 H/N. 由定义直接证明 $H=N_G(M)$.

(2) 和 (3) 由定义直接验证. ■

1.5.5. 设 M 和 N 分别是群 G 的正规子群. 如果 $M\bigcap N=1$, 则对任意 $a\in M,b\in N$ 有 $ab=ba$.

证 设 $a\in M,b\in N$. 因 $aba^{-1}b^{-1}=(aba^{-1})b^{-1}\in N$, $aba^{-1}b^{-1}=a(ba^{-1}b^{-1})\in M$. 故 $aba^{-1}b^{-1}\in M\bigcap N=1$, 即 $ab=ba$. ■

1.5.6. 设 $N\lhd G$, g 是群 G 的任意一个元. 若 g 的阶和 $|G/N|$ 互素, 则 $g\in N$.

证 设 $o(g)=n$, 则 $g^n=1$, $\overline{g}^n=\overline{1}$. 令 $m=|G/N|$, 则 $\overline{g}^m=\overline{1}$. 但是 $(m,n)=1$, 故 $\overline{g}=\overline{1}$. 即 $g\in N$. ■

1.5.7. 如果 $G/Z(G)$ 是循环群, 则 G 是 Abel 群.

证 设 $G/Z(G)=\langle gZ(G)\rangle$. 则 $\forall a,\ b\in G$,存在 $c,\ d\in Z(G)$ 使得 $a=g^mc$, $b=g^nd$. 由此可见 $ab=ba$. 即 G 是 Abel 群. ■

1.5.8*. 用 $I(G)$ 表示 G 的全部内自同构组成的集合. 试证:$I(G)\leqslant \operatorname{Aut}(G)$, 且 $I(G)\cong G/Z(G)$.

证 容易验证 $I(G)$ 是 $\operatorname{Aut}(G)$ 的子群. 考虑映射 $\pi:G\longrightarrow \operatorname{Aut}(G)$, $\pi(g)=\sigma_g$, $\forall g\in G$, 其中 $\sigma_g(x)=gxg^{-1}$, $\forall x\in G$, 则直接验证 π 是群同态而且 $\pi(G)=I(G)$. 因为 $\operatorname{Ker}\pi=Z(G)$, 故由群同态基本定理可知 $I(G)\cong G/Z(G)$. ■

1.5.9*. 试证非可换群 G 的自同构群 $\operatorname{Aut}(G)$ 不是循环群.

特别地, 若群 G 只有素数个自同构, 则 G 是可换群.

证 否则, G 的内自同构群 $I(G)$ 也是循环群, 即 $G/Z(G)$ 是循环群, 从而 G 是可换群. 矛盾!

若群 G 只有素数个自同构, 则 $\mathrm{Aut}(G)$ 是循环群, 从而 G 必是可换群. ■

1.5.10*. 用 $[G,G]$ 表示群 G 的换位子群, 即由所有换位子 $[g,h]=ghg^{-1}h^{-1}$, $g,h\in G$ 生成的 G 的子群; 记 $G^{(1)}=[G,G]$, $G^{(n)}=[G^{(n-1)},G^{(n-1)}]$, $\forall\ n>1$. 则 $G^{(n)}$ 均是 G 的正规子群, $\forall\ n\geqslant 1$.

证 对 n 用归纳法. 熟知 $G^{(1)}$ 是 G 的正规子群. 设 $n>1, x\in G^{(n)}$, $g\in G$, 则 x 形如 $x=g_1h_1g_1^{-1}h_1^{-1}\cdots g_mh_mg_m^{-1}h_m^{-1}$, 其中 g_i, $h_i\in G^{(n-1)}$, $1\leqslant i\leqslant m$. 于是

$$\begin{aligned}gxg^{-1}&=gg_1h_1g_1^{-1}h_1^{-1}\cdots g_mh_mg_m^{-1}h_m^{-1}g^{-1}\\&=(gg_1g^{-1})(gh_1g^{-1})(gg_1^{-1}g^{-1})(gh_1^{-1}g^{-1})\cdots\\&\quad(gg_mg^{-1})(gh_mg^{-1})(gg_m^{-1}g^{-1})(gh_m^{-1}g^{-1}).\end{aligned}$$

由归纳假设 $G^{(n-1)}$ 是 G 的正规子群, 从而 gg_ig^{-1}, $gh_ig^{-1}\in G^{(n-1)}$, $1\leqslant i\leqslant m$, 于是由上式知 gxg^{-1} 仍是 $G^{(n-1)}$ 的换位子的乘积, 所以 $gxg^{-1}\in G^{(n)}$. 即 $G^{(n)}$ 是 G 的正规子群. ■

1.5.11. 设 $N\lhd G$, $N\bigcap[G,G]=\{1\}$, 则 $N\leqslant Z(G)$.

证 设 $x\in N$, $g\in G$. $gxg^{-1}x^{-1}\in N\bigcap[G,G]=\{1\}$, 从而 $x\in Z(G)$. ■

1.5.12*. 群 G 的非平凡子群 N 称为 G 的极小子群, 如果不存在子群 B 使得 $1\subsetneqq B\subsetneqq N$. 试证:

(1) 整数加法群 $\mathbb{Z}$ 没有极小子群.

(2) 有理数加法群 $\mathbb{Q}$ 既没有极小子群也没有极大子群.

证 (1) $\mathbb{Z}$ 的非平凡子群形式如 $\langle n\rangle$, n 是正整数. 注意到 $\langle n\rangle$ 真包含 $\langle mn\rangle$, $\forall\ m>1$. 故 $\mathbb{Z}$ 无极小子群.

(2) 有理数加法群 $\mathbb{Q}$ 的任意一个非平凡子群 H 含有与整数加法群同构的子群, 从而由 (1) 知 H 不是极小子群. 故 $\mathbb{Q}$ 无极小子群.

下证 $\mathbb{Q}$ 无极大子群. 首先证明 $\mathbb{Q}$ 是由集合

$$P=\left\{\frac{1}{p^r}\ \mid\ p\text{为素数},\ r\geqslant 1\right\}$$

生成. 事实上, 设 $m/n\in\mathbb{Q}$, $n=p_1^{r_1}\cdots p_t^{r_t}$, $p_1,\cdots,p_t$ 是互不相同的素数. 令

$b_i = n/p_i^{r_i}$, 则 $(b_1, \cdots, b_t) = 1$. 故存在整数 a_i 使得 $\sum_{i=1}^{t} a_i b_i = 1$. 于是

$$\sum_{i=1}^{t} a_i m \frac{1}{p_i^{r_i}} = \frac{\sum_{i=1}^{t} a_i b_i m}{n} = \frac{m}{n}.$$

这就证明了 $\mathbb{Q} = \langle P \rangle$.

设 H 是 $\mathbb{Q}$ 的真子群, 由上述可知存在素数 p 和正整数 r 使得 $\frac{1}{p^r} \notin H$. 若 H 极大, 则 $\langle H,\ 1/p^r \rangle = \mathbb{Q}$. 于是存在整数 n 使得 $1/p^{r+1} - n/p^r \in H$, 即 $(np-1)/p^{r+1} \in H$. 但 $(np-1, p^{r+1}) = 1$, 故有整数 c, d 使得 $c(np-1)+dp^{r+1} = 1$. 从而

$$\frac{1}{p^{r+1}} = c\frac{np-1}{p^{r+1}} + d\frac{p^{r+1}}{p^{r+1}} \in H.$$

这与 $\frac{1}{p^r} \notin H$ 相矛盾! 这就证明了 $\mathbb{Q}$ 无极大子群. ■

1.5.13*. 设 α 是有限群 G 的自同构, 令 $I = \{g \in G \mid \alpha(g) = g^{-1}\}$. 试证:

(1) 若 $|I| > \frac{3}{4}|G|$, 则 G 是 Abel 群.

(2) 若 $|I| = \frac{3}{4}|G|$, 则 G 一定有指数为 2 的 Abel 正规子群.

证 对于任一 $x \in I$, 有 $xI \bigcap I \subseteq C_G(x)$. 从而 $|xI \bigcap I| \leqslant |C_G(x)|$.
(事实上, $\forall z \in xI \bigcap I$, 有 $y \in I$ 使得 $z = xy$. 于是

$$x^{-1}y^{-1} = \alpha(x)\alpha(y) = \alpha(xy) = \alpha(z) = z^{-1} = y^{-1}x^{-1},$$

即 x 与 y 可换, 从而 z 与 x 可换, 即 $z \in C_G(x)$.)

(1) 设 $|I| > \frac{3}{4}|G|$, 则对任一 $x \in I$ 我们有

$$|xI \bigcap I| = |xI| + |I| - |xI \bigcup I| > \frac{3}{4}|G| + \frac{3}{4}|G| - |G| = \frac{1}{2}|G|,$$

从而 $|C_G(x)| > \frac{1}{2}|G|$. 由 Lagrange 定理知 $C_G(x) = G$, 即 $x \in Z(G)$, 从而 $I \subseteq Z(G)$. 因 $|I| > \frac{3}{4}|G|$, 故 $Z(G) = G$, 即 G 是 Abel 群.

(2) 设 $|I| = \frac{3}{4}|G|$, 则对任一 $x \in I$ 我们有

$$\frac{1}{2}|G| \leqslant |xI \bigcap I| \leqslant |C_G(x)|.$$

我们断言: 存在 $x \in I$ 使得 $|C_G(x)| = \dfrac{1}{2}|G|$. 否则 $C_G(x) = G$, $\forall x \in I$, 即 $I \subseteq Z(G)$. 于是 $|Z(G)| \geqslant |I| = \dfrac{3}{4}|G|$, 故 $Z(G) = G$, 即 G 是 Abel 群, 从而 I 是 G 的子群. 这与 $|I| = \dfrac{3}{4}|G|$ 相矛盾!

设 $x \in I$, 满足 $|C_G(x)| = \dfrac{1}{2}|G|$. 此时 $xI \bigcap I = C_G(x)$ 是 G 的指数为 2 的正规子群. 设 $z, z' \in C_G(x)$, 则 $zz' \in C_G(x)$, 从而 $zz' \in I$. 于是

$$z^{-1}z'^{-1} = \alpha(z)\alpha(z') = \alpha(zz') = (zz')^{-1} = z'^{-1}z^{-1}.$$

即 $C_G(x)$ 是 Abel 群. ■

§6　置　换　群

知识要点:

变换群的重要性; Cayley 定理; S_n 中元的表达、奇偶性、阶.

对称群与交错群的生成系; S_n 中共轭类的划分: 两个置换在 S_n 的同一共轭类中当且仅当它们的型相同.

有限单群; A_n $(n \geqslant 5)$ 的单性; 举例: S_n 的正规子群; S_4/K_4 同构于 S_3.

1.6.1. 把置换 $\sigma = (4\,5\,6)(5\,6\,7)(7\,6\,1)$ 写成不相交轮换的积.

解　$\sigma = (1\,6)(4\,5)$. ■

1.6.2. 讨论置换

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$$

的奇偶性.

解　当 $n = 2m,\ m \geqslant 1$ 时, $\sigma = (1\quad n)(2\quad n-1)\cdots(m\quad m+1)$;

当 $n = 2m-1,\ m \geqslant 1$ 时, $\sigma = (1\quad n)(2\quad n-1)\cdots(m-1\quad m+1)$.

故当 $n = 4m-3,\ 4m,\ m \geqslant 1$ 时, σ 是偶置换; 而当 $n = 4m-2,\ 4m-1,\ m \geqslant 1$ 时, σ 是奇置换. ■

1.6.3.　一个置换的阶等于它的轮换表示中各个轮换因子的长度的最小公倍数.

证　首先, 长为 l 的轮换的阶恰为 l; 其次, 在一个群中, 若 a 的阶为 s, b 的阶为 t, 且 $ab = ba$, 则 ab 的阶恰为 s 与 t 的最小公倍数. 由此即得结论. ■

1.6.4. 设 $\sigma = (1\,2\,\cdots\,n) \in S_n$, 证明: $C_{S_n}(\sigma) = \langle\sigma\rangle$.

证 $C_{S_n}(\sigma)=\{\tau\in S_n\mid \sigma\tau=\tau\sigma\}\supseteq\langle\sigma\rangle$. 另一方面 $\tau\sigma\tau^{-1}=(\tau(1)\,\tau(2)\,\cdots\,\tau(n))$. 因此, 若 $\tau\in C_{S_n}(\sigma)$, 则 $(\tau(1)\,\tau(2)\,\cdots\,\tau(n))=(1\,2\,\cdots\,n)=\sigma$. 设 $\tau(1)=i$, 则

$$\tau=\begin{pmatrix}1 & 2 & \cdots & n-i+1 & n-i+2 & \cdots & n\\ i & i+1 & \cdots & n & 1 & \cdots & i-1\end{pmatrix},$$

即 $\tau=\sigma^{i-1}$. 故 $C_{S_n}(\sigma)=\langle\sigma\rangle$. ■

1.6.5. 试证当 $n\geqslant 3$ 时, 中心 $Z(S_n)=\{1\}$.

证 设 $\tau\neq 1$, $\tau\in S_n$. 则 τ 至少有一个长为 m 的轮换因子 σ, $m>1$. 不妨设 $\sigma=(1\,2\,\cdots\,m)$, 则由题 1.6.4 知, S_m 中就含有与 σ 不可换的元 (这是因为 $C_{S_m}(\sigma)=\langle\sigma\rangle$, 故 $|C_{S_m}(\sigma)|=m$, 而 $|S_m|=m!$). 因此 S_n 中当然就含有与 τ 不可换的元 (将 S_m 看成 S_n 的子群), 即 $\tau\notin Z(S_n)$. ■

1.6.6. 当 $n\geqslant 3$ 时, 试证 $n-2$ 个 3 轮换 $(1\,2\,3)$, $(1\,2\,4)$, $\cdots$, $(1\,2\,n)$ 是 A_n 的生成元.

证 全体长为 3 的轮换生成 A_n. 故只要证这 $n-2$ 个 3 轮换能生成任何一个 3 轮换.

任取 3 轮换 $(i\,j\,k)$, 若 i,j,k 中含有 1 和 2, 则结论显然成立. 若 i,j,k 中含有 1 和 2 之一, 不妨设 $(i\ j\ k)=(1\ j\ k)$, 则 $(1\ j\ k)=(1\,2\,k)(1\,2\,k)(1\,2\,j)(1\,2\,k)$.

若 i,j,k 中既无 1, 也无 2, 则 $(i\,j\,k)=(1\,2\,i)(1\,2\,i)(1\,2\,k)(1\,2\,j)(1\,2\,j)(1\,2\,i)$.

■

1.6.7. 试证 A_4 没有 6 阶子群.

证 直接计算可知 A_4 有 4 个共轭类: $\{(1)\}$, $\{(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$, $\{(1\,2\,3),(1\,4\,2),(1\,3\,4),(2\,4\,3)\}$, $\{(1\,3\,2),(1\,2\,4),(1\,4\,3),(2\,3\,4)\}$. 由此即知 A_4 的正规子群为 $\{(1)\}$, K_4, A_4.

因为指数为 2 的子群是正规子群, 故 A_4 没有 6 阶子群 (否则, A_4 有 6 阶正规子群, 与上述结论不合). ■

1.6.8. 设 σ_1 和 σ_2 是 S_n 中的两个偶置换. 若 σ_1 和 σ_2 在 S_n 中共轭, 则它们在 A_n 中也一定共轭吗?

解 否! 例如: 在 S_4 中 $(1\,2\,3)$ 与 $(1\,3\,2)$ 的型相同, 故它们在 S_4 中共轭, 但在 A_4 中却不共轭 (参见题 1.6.7). ■

注 关于 S_n 的一个共轭类在 A_n 中的分裂情况可参阅 [FZL], p.64. 虽然那本书上只谈 S_5, 但是使用的方法可以推广到 S_n.

1.6.9*. 确定 S_4 的全部正规子群.

解 注意到 G 的子群 N 是 G 的正规子群当且仅当 N 是 G 的一些共轭类的 (无交) 并.

在 S_n 中, 两个置换共轭当且仅当它们有相同的型. 由此可立即写出 S_4 的全部共轭类如下:

型为 1^4: (1)

型为 $1^2 2^1$: $(1\,2)$, $(1\,3)$, $(1\,4)$, $(2\,3)$, $(2\,4)$, $(3\,4)$

型为 $1^3 3^1$: $(1\,2\,3)$, $(1\,3\,2)$, $(1\,2\,4)$, $(1\,4\,2)$, $(1\,3\,4)$, $(1\,4\,3)$, $(2\,3\,4)$, $(2\,4\,3)$

型为 2^2: $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, $(1\,4)(2\,3)$

型为 4^1: $(1\,2\,3\,4)$, $(1\,2\,4\,3)$, $(1\,3\,2\,4)$, $(1\,3\,4\,2)$, $(1\,4\,2\,3)$, $(1\,4\,3\,2)$.

设 N 是 S_4 的正规子群, $S_4 \neq N \neq \{(1)\}$, 则 $|N| = 12, 8, 6, 4, 3, 2$.

首先, $|N| \neq 6$ (否则, 除去单位元外 N 还有 5 个元. 但对上述共轭类的分析表明 5 个元的集合不可能是一些非中心共轭类的并. 矛盾!). 同理可证 $|N| \neq 8, 3, 2$.

其次, 若 $|N| = 12$, 则 $N = A_4$ (否则, $NA_4 = S_4$. 因此 $S_4/A_4 = NA_4/A_4 \cong N/N \bigcap A_4$. 由此可知, S_4 有 6 阶正规子群 $N \bigcap A_4$, 矛盾!).

最后, 若 $|N| = 4$, 则 $N = K_4 = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ (这是因为 N 是一些共轭类的并. 而 $|N| = 4$, 故 $N = K_4$ 是唯一的选择.).

综上所述, $\{(1)\}$, K_4, A_4, S_4 是 S_4 的全部正规子群. ■

1.6.10*. 试证:

(1) 对称群 S_n 是交错群 A_{2n} 的子群.

(2) 每个有限群均是某个交错群的子群.

证 (1) 将 S_n 中的元写成互不相交的轮换的乘积. 考虑群的嵌入 $S_n \longrightarrow A_{2n}$, 它将每个轮换 σ 映成 $\sigma\sigma'$, 其中 σ' 是将 σ 中 1 改为 $n+1$, 2 改为 $n+2, \cdots$, n 改为 $2n$ 所得的 S_{2n} 中的轮换.

(2) 由 Cayley 定理, 每个 n 阶有限群 G 均是对称群 S_n 的子群, 再由 (1) 知 G 是交错群 A_{2n} 的子群. ■

1.6.11*. S_n 中型为 $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$ 的置换共有 $n!/\prod\limits_{i=1}^{n} i^{\lambda_i} \lambda_i!$ 个, 由此证明

$$\sum_{\lambda} \frac{1}{\prod\limits_{i=1}^{n} i^{\lambda_i} \lambda_i!} = 1,$$

其中 λ 取遍所有的型, 即 λ 取遍所有的数组 $(\lambda_1, \lambda_2, \cdots, \lambda_n)$, λ_i 均为非负整数且满足 $\lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = n$.

证 令 $\mathbb{P}(\lambda_1, \lambda_2, \cdots, \lambda_n)$ 是 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换的集合, $\mathbb{P}_n$ 是 n 个字母 $1, 2, \cdots, n$ 的所有排列的集合. 定义映射 $\pi: \mathbb{P}_n \mapsto \mathbb{P}(\lambda_1, \lambda_2, \cdots, \lambda_n)$ 如下:

$\forall p = (p_1, p_2, \cdots, p_n) \in \mathbb{P}_n$, 令 $\pi(p)$ 是这样的置换: 在排列 p 中, 从左至右前 λ_1 个字母均作为长为 1 的轮换因子, 接下来依次作为 λ_2 个对换因子, 等等, 即

$$\pi(p) = \underbrace{(p_1)\cdots(p_{\lambda_1})}_{\lambda_1}\underbrace{(p_{\lambda_1+1}\,p_{\lambda_1+2})\cdots(p_{\lambda_1+2\lambda_2-1}\,p_{\lambda_1+2\lambda_2})}_{\lambda_2}\cdots.$$

显然 π 是满射. 对任一 $\alpha \in \mathbb{P}(\lambda_1, \cdots, \lambda_n)$, $\pi^{-1}(\alpha)$ 中恰好含有 $\prod\limits_{i=1}^{n} i^{\lambda_i}\lambda_i!$ 个排列 (要看出这一点只要注意到两个事实: 其一, 一个长为 i 的轮换 $(t_1\cdots t_i)$ 有 i 种写法: $(t_1\,t_2\cdots t_i)$, $(t_2\cdots t_i\,t_1)$, $\cdots$, $(t_i\,t_1\cdots t_{i-1})$; 其二, λ_i 个两两不相交的长为 i 的轮换是两两乘积可换的.). 由此可见 $|\pi^{-1}(\alpha)|$ 只与 α 的型相关, 故有

$$|\mathbb{P}_n| = |\pi^{-1}(\alpha)||\mathbb{P}(\lambda_1, \cdots, \lambda_n)|, \quad \forall \alpha \in \mathbb{P}(\lambda_1, \cdots, \lambda_n).$$

即

$$|\mathbb{P}(\lambda_1, \cdots, \lambda_n)| = \frac{n!}{\prod\limits_{i=1}^{n} i^{\lambda_i}\lambda_i!}.$$

当 λ 取遍所有的型时, 有 $\sum\limits_{\lambda}|\mathbb{P}(\lambda_1, \cdots, \lambda_n)| = |S_n|$, 由此即得到所要证的等式. ■

1.6.12*. 当 $n \geqslant 2$ 时, 试证 $(1\,2)$ 和 $(1\,2\,3\cdots n)$ 是 S_n 的一组生成元.

证 设 H_n 是由 $(1\,2)$ 和 $(1\,2\,3\cdots n)$ 生成的 S_n 的子群, 用数学归纳法证明 $H_n = S_n$.

$n=2$ 时显然成立. 设 $H_{n-1} = S_{n-1}$, 我们有

$(2\,3\cdots n) = (1\,2)(1\,2\cdots n) \in H_n$,

$(1\,n) = (n\,n-1\cdots 3\,2\,1)(2\,3\cdots n) = (1\,2\cdots n)^{n-1}(2\,3\cdots n) \in H_n$,

$(1\,2\cdots n-1) = (1\,n)(1\,2\cdots n) \in H_n$.

由归纳假设 $(1\,2)$ 和 $(1\,2\cdots n-1)$ 生成 S_{n-1}. 因此 $H_n \supseteq S_{n-1}$, $(1\,n) \in H_n$. 而 $(1\,2)$, $\cdots$, $(1\,n-1)$, $(1\,n)$ 是 S_n 的一组生成元, 故 $H_n = S_n$. ■

§7 群在集合上的作用

知识要点:

群作用的思想; 群作用的两种定义的等价性; 作用的核; 三种典型的作用及其核: (左) 正则作用、(左) 诱导作用、共轭作用.

轨道公式: 若群 G 作用在集合 S 上, $x \in S$, 则 $|Gx| = \dfrac{|G|}{|G_x|}$, 其中 $G_x = \{g \in G \mid gx = x\}$ (称为 x 的固定子群), $Gx = \{gx \mid g \in G\}$ (称为 x 所在的 G- 轨道).

Klein 关于几何学的 Erlangen 纲领: (欧氏、仿射、射影等) 几何学与 (正交、仿射、射影等) 变换群作用下的不变性.

Burnside 引理及其在计数中的应用 (例如, 项链问题、开关线路问题、正多面体的着色问题、分子结构的计数等).

1.7.1. 设 G 作用在集合 S 上, 对任意 $a, b \in S$, 若存在 $g \in G$ 使得 $ga = b$, 则 $G_a = g^{-1}G_b g$. 换句话说, 同一轨道中元的固定子群彼此共轭.

解 我们有

$$\begin{aligned} G_b &= \{x \in G \,|\, xb = b\} = \{x \in G \,|\, xga = ga\} \\ &= \left\{x \in G \,|\, g^{-1}xga = a\right\} = \left\{x \in G \,|\, g^{-1}xg \in G_a\right\} \\ &= gG_a g^{-1}. \end{aligned}$$

■

1.7.2. 设群 G 在集合 S 上的作用是可迁的, N 是 G 的正规子群, 则 S 在 N 作用下的每个轨道有同样多的元.

解 设 $S = Ga$, 则对任一 $x \in S$, $x = ga$, $g \in G$, 有

$$\begin{aligned} N_x &= \{\, n \in N \,|\, nx = x\} = \{\, n \in N \,|\, nga = ga\} \\ &= \left\{\, n \in N \,|\, g^{-1}ng \in G_a\right\} = N \bigcap gG_a g^{-1}. \end{aligned}$$

又因为 $N \lhd G$, 故 $N_x = N \bigcap gG_a g^{-1} = g(N \bigcap G_a)g^{-1} = gN_a g^{-1}$. 从而

$$|Nx| = \frac{|N|}{|N_x|} = \frac{|N|}{|gN_a g^{-1}|} = \frac{|N|}{|N_a|} = |Na|.$$

即 S 在 N 作用下的每个轨道有同样多的元. ■

1.7.3*. (Burnside 引理) 设群 G 作用在集合 S 上, 令 t 表示 S 在 G 作用下的轨道的条数. 对任意 $g \in G$, $F(g)$ 表示 S 在 g 作用下不动点的个数, 即 $F(g) = |\{x \in S \mid gx = x\}|$. 试证

$$t = \frac{\sum\limits_{g \in G} F(g)}{|G|}.$$

这就是说, G 的每个元作用在 S 上平均使得 t 个文字不动.

证 令 $\Omega = \{(g, x) \in G \times S \mid gx = x\}$, 我们用两种方法计算 $|\Omega|$.

第一种方法: 先固定 $g \in G$, 得到

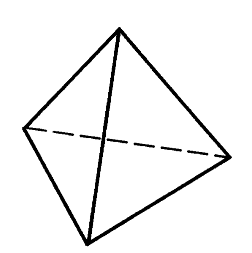
$$|\Omega| = \sum_{g \in G} F(g).$$

第二种方法: 先固定 $x \in S$. 设 $S = \bigcup_{1 \leqslant i \leqslant t} Gx_i$ 是 S 的按轨道的划分. 注意到若 $x \in Gx_i$, 则 $|Gx| = |Gx_i|$. 于是

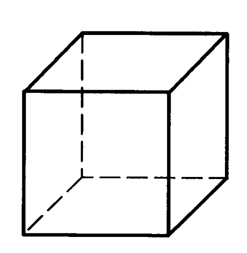
$$\begin{aligned}|\Omega| &= \sum_{x \in S} |G_x| = \sum_{x \in S} \frac{|G|}{|Gx|} = \sum_{i=1}^{t} \sum_{x \in Gx_i} \frac{|G|}{|Gx|} \\ &= \sum_{i=1}^{t} \sum_{x \in Gx_i} \frac{|G|}{|Gx_i|} = \sum_{i=1}^{t} |Gx_i| \frac{|G|}{|Gx_i|} = t|G|.\end{aligned}$$

故 $\sum_{g \in G} F(g) = t|G|$. ■

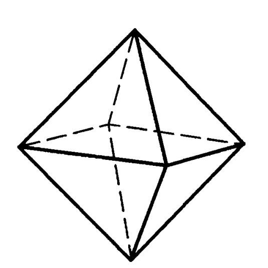
1.7.4. 求正四面体、正六面体、正八面体、正十二面体和正二十面体 (如下图所示) 的旋转群和对称群各有多少个元?



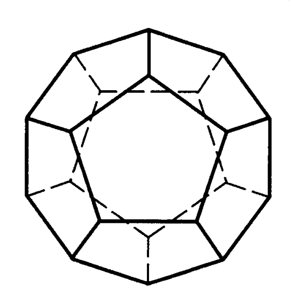
正四面体 (tetrahedron)



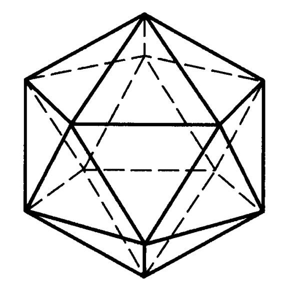
正六面体 (hexahedron)



正八面体 (octahedron)



正十二面体 (dodecahedron)



正二十面体 (icosahedron)

解 设 Σ 是正多面体的顶点的集合, 则相应于五个正多面体, Σ 分别含有 4, 8, 6, 20, 12 个顶点. (**注** 设 v 为顶点数, e 为棱数, f 为面数, 则这五个正多面体的 (v, e, f) 分别为 $(4,6,4)$, $(8,12,6)$, $(6,12,8)$, $(20,30,12)$, $(12,30,20)$. 验证 Euler 公式 $v - e + f = 2$.)

相应的旋转群和对称群在 Σ 上有自然的作用, 且作用是可迁的. 因此由轨道公式知 $|G| = |\Sigma||G_1|$, 其中 G_1 是顶点 1 的固定子群.

若 G 是旋转群, 则 G_1 分别是正三角形、正三角形、正四边形、正三角形、正五边形的旋转群, 因此其阶分别为 3, 3, 4, 3, 5. 故 G 的阶分别为 12, 24, 24, 60, 60.

若 G 是对称群, 则 G_1 分别是正三角形、正三角形、正四边形、正三角形、正五边形的对称群, 故 $|G_1|$ 分别是 6, 6, 8, 6, 10. 故 G 的阶分别是 24, 48, 48, 120, 120. ■

注　注意到正六面体的旋转群和正八面体的旋转群同构; 正六面体的对称群和正八面体的对称群同构. 正十二面体的旋转群与正二十面体的旋转群同构; 正十二面体的对称群与正二十面体的对称群同构.

三维空间中有且仅有上述五个正多面体被认为是整个数学史上最优美、最奇妙的发现之一. 参见 [WH].

1.7.5*. 设 p 是一个素数, G 是 p 的方幂阶的群. 试证 G 的非正规子群的个数一定是 p 的倍数.

证　令 $S = \{G$ 的非正规子群$\}$, 考虑 G 在 S 上的共轭作用. 由轨道公式知

$$|S| = \sum_{H\in R} \frac{|G|}{|G_H|},$$

其中 R 是 S 的一组轨道代表元, G_H 是 H 的固定子群, 也就是 H 在 G 中的正规化子. 因 $|G/G_H|$ 是 p 的方幂, 且 $G \neq G_H$ (否则 $H \lhd G$, 与 $H \in S$ 不合), 故 $p \mid |S|$. ■

1.7.6*. 令 G 是一个单群, 如果存在 G 的真子群 H 使得 $[G:H] \leqslant 4$, 则 $|G| \leqslant 3$.

证　考虑 G 在 H 的左陪集集合上的左诱导作用. 于是有群同态 $\rho: G \to S_m$, 其中 $m = [G:H] \leqslant 4$. 因 G 是单群, 故 $\operatorname{Ker}\rho = \{1\}$ (否则 $\operatorname{Ker}\rho = G$, 从而 $H = G$), 于是 G 可视为 S_m 的子群, $m \leqslant 4$.

若 $m = 3$, 因 G 是单群, 故 $G \neq S_3$, 从而 $|G| \leqslant 3$.

若 $m = 4$, 因 G 是单群, 故 $G \neq S_4$, $G \neq A_4$. 又因为 p- 群有非平凡的中心, 故 $|G| \neq 8$. 因 $[G:H] = 4$, 故 $|G| \neq 6$. 又因为 4 阶群非单, 从而 $|G| \leqslant 3$. ■

1.7.7*. 设 H 是群 G 的指数为 $n < \infty$ 的真子群, 试证 H 一定含有 G 的一个有有限指数的真正规子群.

如果还有 $|G| > n!$, 则 G 不是单群.

证　设 $n = [G:H]$. 考虑 G 在 H 的左陪集集合上的左诱导作用, 则有群

同态

$$\rho:\ G \longrightarrow S_n, \quad \operatorname{Ker}\rho = \bigcap_{g\in G} gHg^{-1} \lhd G.$$

因 $\operatorname{Ker}\rho \leqslant H \neq G$, 故 $\operatorname{Ker}\rho \neq G$. 因

$$G/\operatorname{Ker}\rho \cong \operatorname{Im}(\rho) \leqslant S_n,$$

故 $[G:\operatorname{Ker}\rho]\,|\,n!$. 从而 $\operatorname{Ker}\rho$ 是 G 的指数有限的真正规子群且 $\operatorname{Ker}\rho \subseteq H$.

如果还有 $|G| > n!$, 则 $\operatorname{Ker}\rho \neq \{1\}$, 从而 G 不是单群. ■

1.7.8*. 试证一般线性群 $GL(n,\mathbb{C})$ 不含有指数有限的真子群.

证 否则, 设 H 是 $G = GL(n,\mathbb{C})$ 的指数有限的真子群, $[GL(n,\mathbb{C}):H] = m$. 考虑 G 在 H 的左陪集集合上的左诱导作用, 则有群同态 $\rho:\ G \longrightarrow S_m$. 于是 $|G/\operatorname{Ker}\rho|\ |\ m!$. 设 $|G/\operatorname{Ker}\rho| = s$.

$\forall B \in G$, 有 $B^s \in \operatorname{Ker}\rho$. 而另一方面, 由线性代数知对于任一 $A \in G$ 和任一正整数 t, 存在 $B \in G$ 使得 $A = B^t$. 因此 $A \in \operatorname{Ker}\rho$, $\forall A \in G$. 于是 $G = \operatorname{Ker}\rho$, 即 $H = G$, 矛盾! ■

注 下证线性代数中的结论: 设 A 是复可逆方阵, 则对任意正整数 t, 均存在复可逆方阵 B 使得 $A = B^t$.

不妨设 A 是 Jordan 块 $J_n(\lambda)$, $\lambda \neq 0$, 即

$$A = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & & \\ & & & & 1 \\ & & & & \lambda \end{pmatrix}.$$

对 n 用归纳法. 记 $A = \begin{pmatrix} \lambda & \alpha \\ 0 & C \end{pmatrix}$, $\quad C = J_{n-1}(\lambda)$, $\quad \alpha = (1, 0, \cdots, 0)$. 由归纳假设, 对任意正整数 t, 存在上三角复可逆方阵 D, 使得 $C = D^t$. 令 $B = \begin{pmatrix} a & \beta \\ 0 & D \end{pmatrix}$, 其中 $a = \sqrt[t]{\lambda}$, β 待定, 欲使 $B^t = A$, 即 $A = \begin{pmatrix} \lambda & \alpha \\ 0 & C \end{pmatrix} = \begin{pmatrix} \lambda & \gamma \\ 0 & C \end{pmatrix}$, 其中 $\gamma = \beta \sum_{i=0}^{t} a^i D^{t-i}$. 这归结为解线性方程组

$$\beta \sum_{i=0}^{t} a^i D^{t-i} = \alpha,$$

或者

$$\sum_{i=0}^{t} a^i (D^{\mathrm{Tr}})^{t-i} \beta^{\mathrm{Tr}} = \alpha^{\mathrm{Tr}},$$

这里 D^{Tr} 是 D 的转置矩阵. 这是一个系数矩阵为

$$\begin{pmatrix} \lambda & & & & \\ * & & & & \\ * & * & \ddots & & \\ * & * & * & & \\ * & * & * & * & \lambda \end{pmatrix}$$

的 $n-1$ 阶下三角矩阵线性方程组. 因为系数矩阵的秩为 $n-1$, 从而必有唯一解. ■

1.7.9*. 求对称群 S_3 的自同构群 $\mathrm{Aut}(S_3)$.

解 令 $\Sigma = \{S_3 \text{ 的 2 阶子群}\} = \{A_1, A_2, A_3\}$. 考虑 $G = \mathrm{Aut}(S_3)$ 在 Σ 上的自然作用, 于是有群同态 $\rho\colon\ G \longrightarrow S_3$. 因为

$$\begin{aligned} \mathrm{Ker}\,\rho &= \{\alpha \in \mathrm{Aut}(S_3) \mid \alpha(A_i) = A_i,\ i = 1,2,3\} \\ &= \{\alpha \in \mathrm{Aut}(S_3) \mid \alpha((12)) = (12),\ \alpha((13)) = (13),\ \alpha((23)) = (23)\} \\ &= \{1\}, \end{aligned}$$

故 $G \leqslant S_3$. 另一方面 S_3 的内自同构群 $I(S_3)$ 同构于 $S_3/Z(S_3) = S_3$. 于是 $G \cong S_3$. ■

1.7.10*. 令 G 是阶数为 $2^n m$ 的群, 其中 m 是奇数. 如果 G 含有一个 2^n 阶的元, 则 G 含有一个指数为 2^n 的正规子群.

证 对 n 用数学归纳法. 下述证明也包含了对 $n=1$ 情形的证明. 设 $g \in G$ 且 $o(g) = 2^n$, 考虑 G 的左正则作用. 于是有群的单同态 $\rho\colon\ G \longrightarrow S(G) = S_{2^n m}$. 于是 $\rho(g)$ 的阶也为 2^n. 将 $\rho(g)$ 写成互不相交的轮换之积. 因为对任一 $a \in G$, G 中的 2^n 个元 $a, \rho(g)a, \rho(g^2)a, \cdots, \rho(g^{2^n-1})a$ 互不相同, 故 $\rho(g)$ 的每个轮换因子长为 2^n. 又因 $\rho(g)$ 将 G 的每个元都变动, 从而 $\rho(g)$ 是 m 个长为 2^n 的轮换之积. 于是 $\rho(g)$ 是奇置换, 从而 $N = \rho(G) \bigcap A_{2^n m}$ 是 $\rho(G)$ 的指数为 2 的正规子群, 从而 $|N| = 2^{n-1}m$. 由归纳假设知, N 有正规子群 M 使得 $[N:M] = 2^{n-1}$. 于是 $[G:M] = 2^n$, $|M| = m$.

下证 $M \lhd G$. 否则存在 $g \in G$ 使得 $gMg^{-1} \neq M$. 设 $x = gag^{-1} \notin M$, $a \in M$, 则 $x \in gNg^{-1} = N$, $\overline{x} \neq \overline{1} \in N/M$. 故 $\overline{x}$ 的阶为 2 的正次幂. 但是

$$\overline{x}^m = \overline{ga}^m \overline{g}^{-1} = \overline{1},$$

于是 $o(\bar{x}) \mid m$. 矛盾! ■

1.7.11*. 设 α 是有限群 G 的一个自同构. 若 α 把每个元都变到它在 G 中的共轭元, 即对任意 $g \in G$, g 和 $\alpha(g)$ 共轭, 则 α 的阶的每个素因子都是 $|G|$ 的因子.

证 设 $o(\alpha) = pm$, p 为素数, 则 $o(\alpha^m) = \dfrac{pm}{(m, pm)} = p$. 因为 $\alpha^m(g)$ 和 g 也共轭, $\forall g \in G$, 故不妨设 $o(\alpha) = p$. 对每一 $x \in G$, 令 $[x] = \{gxg^{-1} \mid g \in G\}$.

断言: 存在共轭类 $[x]$, 使得 $[x]$ 中不含 α 的不动点.

否则, 即任意共轭类 $[x]$ 均有 α 的不动点. 因 α 的不动点全体作成的子群 $H \neq G$ (这是因为 $o(\alpha) = p$), 从而真子群 H 的共轭子群覆盖了 G. 矛盾!

设 $[x]$ 中不含 α 的不动点. 因 $o(\alpha) = p$, 故 $[x]$ 中也不含 α^i 的不动点, $i = 1, \cdots, p-1$. 设 $a \in [x]$. 考虑 $\langle\alpha\rangle$ 在 $[x]$ 上的自然作用. 因为 a 不是 α^i 的不动点, $i = 1, \cdots, p-1$, 故 a 的固定子群 $\langle\alpha\rangle_a$ 为 $\{1\}$. 从而

$$|\langle\alpha\rangle a| = \frac{|\langle\alpha\rangle|}{|\langle\alpha\rangle_a|} = |\langle\alpha\rangle| = p.$$

因为 $[x] = \bigcup_a \langle\alpha\rangle a$, 故 $p \mid |[x]| \mid |G|$. ■

1.7.12*. 设 p 是 $|G|$ 的最小素因子. 若 p 阶子群 $A \lhd G$, 则 $A \leqslant Z(G)$.

特别地, p- 群 G 的 p 阶正规子群含于 G 的中心.

证 因为 $A \lhd G$, 故 G 在 A 上有共轭作用. 于是得到群同态 $\rho: G \longrightarrow S(A) = S_p$. 注意到 $\rho(G) \subseteq \mathrm{Aut}(A) = \mathbb{Z}_{p-1}$ 且 $\mathrm{Ker}\,\rho = C_G(A)$, 于是 $|G/C_G(A)| = |\mathrm{Im}\rho| \mid (p-1)$. 但是 $|G/C_G(A)|$ 是 $|G|$ 的因子, 而 p 是 $|G|$ 的最小素因子, 故只能 $|G/C_G(A)| = 1$, 即 $C_G(A) = G$, 即 $A \leqslant Z(G)$. ■

§8 Sylow 定理

知识要点:

Lagrange 定理之逆不成立: 有限群 G 未必有 d 阶子群, 其中 d 是 $|G|$ 的正因子. 但是有如下 Sylow 定理. 设 p 为素数, G 是有限群, 则

1. 设 $p^k \mid |G|$, 则 G 的阶为 p^k 的子群的个数模 p 同余于 1; 特别地, G 有 p^k 阶子群.

设 $|G| = p^n m$, 其中 $n \geqslant 1$, $p \nmid m$, 则 G 的 p^n 阶子群称为 G 的 Sylow p- 子群.

2. G 的 Sylow p- 子群是互相共轭的.

因此, G 的 Sylow p- 子群个数等于 $[G : N_G(P)]$, 其中 P 是 G 的任一 Sylow p- 子群, $N_G(P)$ 是 P 在 G 中的正规化子. 从而, G 的 Sylow p- 子群 P 是正规子群当且仅当 $[G : N_G(P)] = 1$.

注意 $[G:N_G(P)]$ 是 $|G|$ 的因子, 而且模 p 同余于 1.

3. G 的任一阶为 p^k 的子群必包含于 G 的某一 Sylow p- 子群.

利用 Sylow 子群可能是正规的, 经常能判断有限群的非单性: 例如, pq 阶群和 p^2q 阶群均非单群, 其中 p,q 均为素数.

阶数最小的非可交换的单群是交错群 A_5.

1.8.1. 设 p 是 $|G|$ 的素因子, 则 G 有 p 阶元.

证 由 Sylow 定理 G 有 p 阶子群, 从而 G 有 p 阶元. ■

1.8.2. 设 p 是 $|G|$ 的素因子, 则方程 $x^p=1$ 在 G 中的解的个数是 p 的倍数.

证 $x^p=1$ 在 G 中的解都落在 G 的某一 p 阶子群中, 而由 Sylow 定理, G 的 p 阶子群的个数为 $kp+1$, 其中 k 为某一非负整数. 因此 G 有 $(kp+1)(p-1)=(kp+1)p-kp-1$ 个 p 阶元, 于是 $x^p=1$ 在 G 中有 $(kp+1)p-kp$ 个解. ■

1.8.3. 证明 6 阶非 Abel 群只有 S_3.

证 $|G|=2\times 3$, 故 G 有 3 阶正规子群 $A=\langle\beta\rangle$. 设 $H=\langle\alpha\rangle$ 是 G 的一个 2 阶子群, 则 $G=AH$. 因 G 不可交换, 故 α 与 β 不可交换, 即 $\alpha\beta\alpha^{-1}\neq\beta$, 从而 $\alpha\beta\alpha^{-1}=\beta^2$. 容易验证

$$(1\ 2)\mapsto\alpha,\ (1\ 2\ 3)\mapsto\beta$$

就给出了群同构 $G\cong S_3$. ■

1.8.4. 200 阶群有正规的 Sylow 子群.

证 $200=2^3 5^2$. Sylow 5- 子群的个数 $N(25)$ 为 $(5k+1)$ 且整除 8, 其中 k 为某一非负整数, 故 $N(25)=1$, 即 25 阶子群是正规的 Sylow 子群. ■

1.8.5. 确定 S_4 的 Sylow 子群的个数.

解 $|S_4|=2^3 3$. S_4 的 Sylow 3- 子群个数 $N(3)=(3k+1)|8$, 基中 k 为某一非负整数. 而 S_4 至少有 4 个 Sylow 3- 子群, 即 3- 轮换生成的子群, 故 $N(3)=4$. 而 $N(8)=(2k+1)|3$, 但 S_4 无 8 阶正规子群, 故 $N(8)=3$.

事实上, S_4 的 Sylow 3- 子群为

$$\langle(123)\rangle,\quad \langle(124)\rangle,\quad \langle(134)\rangle,\quad \langle(234)\rangle.$$

而其 Sylow 2- 子群为

$$\{1,\ (13),\ (24),\ (12)(34),\ (13)(24),\ (14)(23),\ (1234),\ (1432)\},$$

$$\{1,\ (12),\ (34),\ (12)(34),\ (13)(24),\ (14)(23),\ (1324),\ (1423)\},$$

$$\{1,\ (14),\ (23),\ (12)(34),\ (13)(24),\ (14)(23),\ (1243),\ (1342)\}.$$

■

1.8.6. 设 P 是有限群 G 的 Sylow p- 子群, $N_G(P) \lhd G$. 证明 $P \lhd G$.

证 对任一 $g \in G$, P 与 gPg^{-1} 均是 $N_G(P)$ 的 Sylow p- 子群. 故由 Sylow 定理知, 它们在 $N_G(P)$ 中共轭, 即有 $n \in N_G(P)$ 使得 $gPg^{-1} = nPn^{-1} = P$. 即 $P \lhd G$. ■

1.8.7. 设 N 是有限群 G 的正规子群. 若素数 p 和 $|G/N|$ 互素, 则 N 包含 G 的所有 Sylow p- 子群.

证 因为 $|G|=|G/N||N|$ 及 p 与 $|G/N|$ 互素, 故 N 的 Sylow p- 子群也是 G 的 Sylow p- 子群. 设 P 是 N 的一个 Sylow p- 子群, P' 是 G 的任一 Sylow p- 子群. 则由 Sylow 定理知 $P' = gPg^{-1} \leqslant gNg^{-1} = N$. ■

1.8.8. 设 N 是有限群 G 的正规子群, P 是 G 的 Sylow p- 子群. 则

(1) $N \bigcap P$ 是 N 的 Sylow p- 子群.

(2) PN/N 是 G/N 的 Sylow p- 子群.

(3) $(N_G(P)N)/N = N_{G/N}(PN/N)$.

证 因 $N \lhd G$, 故 $NP = PN$ 是 G 的子群且

$$[N : N \bigcap P] = [NP : P].$$

由此即看出 (1) (注意上式并非从同构定理得到, 而是从两个子群的积集计数公式得到).

而 $[G/N : PN/N] = [G : PN]$ 整除 $[G : P]$, 由此可以看出 (2).

(3) 由定义易知 $(N_G(P)N)/N \subseteq N_{G/N}(PN/N)$. 设 $N_{G/N}(PN/N) = T/N$, $T \leqslant G$. 则由定义易知 $tPt^{-1} \subseteq PN$, $\forall\, t \in T$. 从而 P 和 tPt^{-1} 均是 PN 的 Sylow p- 子群, 故由 Sylow 定理知 P 和 tPt^{-1} 在 PN 中共轭. 由此推得 $t \in N_G(P)N$, 即 $T \subseteq N_G(P)N$. ■

1.8.9. 设 G 是集合 Σ 上的置换群, P 是 G 的 Sylow p- 子群, $a \in \Sigma$. 若 $p^m \mid |Ga|$, 则 $p^m \mid |Pa|$.

证 注意到固定子群 P_a 恰好是固定子群 G_a 与 P 的交, 故由轨道公式知

$$|Ga|\frac{|G_a|}{|G_a \bigcap P|} = \frac{|G|}{|G_a|}\frac{|G_a|}{|P_a|} = \frac{|G|}{|P_a|} = \frac{|G|}{|P|}\frac{|P|}{|P_a|} = [G : P]|Pa|.$$

因 $p^m \mid |Ga|$, 故 $p^m \mid ([G : P]|Pa|)$. 但是 p 与 $[G : P]$ 互素, 故 $p^m \mid |Pa|$. ■

1.8.10. 确定恰有 3 个共轭类的有限非交换群 G.

证 设 G 的 3 个共轭类的阶分别为 $1, m, n$, 其中 $1 \leqslant m \leqslant n$, 则 $|G| = 1 + m + n$.

首先 $m \neq n$: 否则 $m \mid |G| = 2m+1$, 从而 $m=1$, 于是 G 可换. 与题设矛盾. 再由 $m<n$ 和 $n \mid |G| = 1+m+n$ 知 $n=m+1$. 从而 $m \mid |G| = 2m+2$, 故 $m=1,2$. 因 4 阶群可换, 故 $m=2$, $|G|=6$. 从而 $G \cong S_3 \cong D_3$. ■

1.8.11*. 设 P 是有限群 G 的 Sylow p- 子群, H 是 G 的子群, $p \mid |H|$. 则存在 $a \in G$ 使得 $aPa^{-1} \bigcap H$ 是 H 的 Sylow p- 子群.

证 因为 $p \mid |H|$, 故可取到 H 的 Sylow p- 子群 A. 由 Sylow 定理知, A 含于 G 的某个 Sylow p- 子群 aPa^{-1}, 从而 $A \subseteq aPa^{-1} \bigcap H$. 而 $aPa^{-1} \bigcap H$ 是 H 的阶为 p 的幂的子群, 故 $|aPa^{-1} \bigcap H| \leqslant |A|$. 于是 $A = aPa^{-1} \bigcap H$, 即 $aPa^{-1} \bigcap H$ 是 H 的 Sylow p- 子群. ■

1.8.12. 24, 36, 48 阶群均非单群.

证 设 $|G| = 24 = 2^3 \times 3$. 不妨设 G 的 Sylow 2- 子群非正规. 则由 Sylow 定理知, G 有 3 个 Sylow 2- 子群 P_1, P_2, P_3. 考虑 G 在 $\{P_1, P_2, P_3\}$ 上的共轭作用, 它诱导了群同态 $\rho: G \longrightarrow S_3$.

易知 $\mathrm{Ker}\rho \neq \{1\}$ (否则 $\rho: G \longrightarrow S_3$ 是单射. 这不可能: 因为 $|G| = 24$, $|S_3| = 6$).

又易知 $\mathrm{Ker}\rho \neq G$ (否则 $gP_ig^{-1} = P_i$, $\forall\, g \in G$, $i=1,2,3$. 这与 G 的 Sylow 2- 子群互相共轭不合).

因此 $\mathrm{Ker}\rho$ 是 G 的非平凡的正规子群, 从而 G 非单群.

同理可证 36, 48 阶群非单群. ■

1.8.13*. 确定 S_4 的自同构群 $\mathrm{Aut}(S_4)$.

解 令 $\Sigma = \{P_1,\ P_2,\ P_3,\ P_4\}$ 是 S_4 的 Sylow 3- 子群的集合, 即

$$\Sigma = \{\langle(123)\rangle,\ \langle(124)\rangle,\ \langle(134)\rangle,\ \langle(234)\rangle\}.$$

令 $G = \mathrm{Aut}(S_4)$. 因为 S_4 的中心为 1, 故 S_4 的内自同构群 $I(S_4)$ 同构于 S_4, 从而 $|G| \geqslant 24$.

因为 S_4 的自同构将 Sylow 3- 子群仍变成 Sylow 3- 子群, 故 G 在 Σ 上有自然的作用, 这个群作用诱导出群同态 $\pi:\ G \longrightarrow S_4$, 从而得到

$$\mathrm{Ker}\,\pi = \{\alpha \in G \mid \alpha(P_i) = P_i,\ i=1,2,3,4\}.$$

我们断言 $\mathrm{Ker}\,\pi = \{1\}$, 从而由 $|G| \geqslant 24$ 知 $G \cong S_4$.

设 $\alpha \in \mathrm{Ker}\,\pi$. 因为 α 将 S_4 的 12 阶子群仍变成 12 阶子群, 故 $\alpha(A_4) = A_4$.

又 α 将 2 阶元变成 2 阶元, 故 α 将 S_4 中的对换变成对换, 或变成两个文字不相交的对换的乘积. 但两个文字不相交的对换的乘积属于 A_4, 由 $\alpha(A_4) = A_4$ 知, α 只能将 S_4 中的对换变成对换.

因 $\alpha(\langle(123)\rangle) = \langle(123)\rangle$, 故 $\alpha((123)) = (123)$, 或者 $\alpha((123)) = (132)$. 因 $(123) = (13)(12)$, 故 $\alpha((12))$ 只能是 (12), 或者 (13), 或者 (23).

因 $\alpha(\langle(124)\rangle) = \langle(124)\rangle$, 故 $\alpha((124)) = (124)$, 或者 $\alpha((124)) = (142)$. 因 $(124) = (14)(12)$, 故 $\alpha((12))$ 只能是 (12), 或者 (14), 或者 (24).

综合起来 $\alpha((12))$ 只能是 (12).

同理 $\alpha((13)) = (13)$, $\alpha((14)) = (14)$. 因 (12), (13), (14) 生成 S_4, 故 $\alpha = \mathrm{id}$. ■

1.8.14*. 设 $P_1, \cdots, P_t$ 是有限群 G 的全部 Sylow p- 子群. 若对 $i \neq j$, $1 \leqslant i \leqslant t, 1 \leqslant j \leqslant t$, 总有 $[P_i : P_i \bigcap P_j] \geqslant p^r$, 则 $t \equiv 1 (\mathrm{mod}\ p^r)$.

证 令 $P := P_1$, $N := N_G(P)$, 则 $t = [G : N]$. 考虑 G 关于 (N, P) 的双陪集分解

$$G = \bigcup_{1 \leqslant i \leqslant m} Na_iP, \quad \text{其中 } a_1 = 1.$$

对任一双陪集 NaP, 记

$$s(a) := \frac{|NaP|}{|N|} = \frac{|P|}{|P \bigcap aNa^{-1}|},$$

则

$$s(a) = 1 \Longleftrightarrow aNa^{-1} \supseteq P \Longleftrightarrow a^{-1}Pa \subseteq N.$$

此时, 因 P 与 $a^{-1}Pa$ 均是 N 的 Sylow p- 子群, 故它们在 N 中共轭. 从而 $s(a) = 1 \Longleftrightarrow a \in N$. 于是

$$t = 1 + \sum_{i=2}^{m} |Na_iP| = 1 + \sum_{i=2}^{m} \frac{|P|}{|N \bigcap a_i^{-1}Pa_i|}.$$

因 $N \bigcap a_i^{-1}Pa_i$ 是 p 群, 故由 Sylow 定理知 $N \bigcap a_i^{-1}Pa_i$ 含于 N 的某一 Sylow p- 子群 P' 中. P' 也是 G 的 Sylow p- 子群, 从而

$$N \bigcap a_i^{-1}Pa_i = P' \bigcap a_i^{-1}Pa_i.$$

于是由假设 $\dfrac{|P|}{|N \bigcap a_i^{-1}Pa_i|} \geqslant p^r$, $i = 2, \cdots, m$. 从而 $t \equiv 1\ (\mathrm{mod}\ p^r)$. ■

1.8.15*. 设 G 是集合 Σ 上的置换群, $a \in \Sigma$, P 是固定子群 G_a 的 Sylow p- 子群, $\triangle$ 是轨道 Ga 在 P 作用下的全部不动点的集合. 证明 $N_G(P)$ 在 $\triangle$ 上的作用是可迁的.

证 $\triangle = \{ga \in Ga \mid pga = ga,\ \forall p \in P\}$. 对任一 $n \in N_G(P)$ 和 $ga \in \triangle$, 有

$$p(nga) = np'ga = nga, \ \forall p \in P,$$

其中 $p'=n^{-1}pn\in P$. 这表明 $N_G(P)$ 在 $\triangle$ 上有自然的作用. 因

$$\triangle=\{ga\in Ga\mid g^{-1}Pg\leqslant G_a\},$$

从而 P 与 $g^{-1}Pg$ 都是 G_a 的 Sylow p- 子群, 故它们在 G_a 中共轭, 即 $g^{-1}Pg=h^{-1}Ph,\ h\in G_a$. 于是 $g\in N_G(P)G_a$, 即

$$\triangle=\{ga\in G_a\mid g\in N_G(P)G_a\}=N_G(P)G_aa=N_G(P)a,$$

即 $N_G(P)$ 在 $\triangle$ 上的作用是可迁的. ■

1.8.16*. 设 G 是 24 阶群且中心 $Z(G)=1$, 证明 $G\cong S_4$.

证　因 $24=2^33$, 故 G 的 Sylow 3- 子群个数 $N(3)=(3k+1)\mid 8$. 首先断言 $N(3)=4$.

否则, $N(3)=1$. 设 $T=\langle t\rangle$ 是 G 的 3 阶正规子群.

① 若 G 的 Sylow 2- 子群的个数 $N(8)=1$, 则 G 有 8 阶正规子群 E, 从而 $G=TE$. 因 $T,E\lhd G$, $T\bigcap E=\{1\}$, 故 T 中任一元与 E 中任一元可交换. 从而 $T\leqslant Z(G)$. 矛盾.

② 因此 $N(8)=3$. 设 E 是 G 的一个 Sylow 2- 子群, 则 $G=TE$. 于是 G 的 3 个 Sylow 2- 子群为 E, tEt^{-1}, t^2Et^{-2}. 考虑 G 在 E 的左陪集空间上的左诱导作用, 故有群同态 $\pi:\ G=TE\longrightarrow S_3$. 则 $N:=\operatorname{Ker}\pi=\bigcap\limits_{0\leqslant i\leqslant 2}t^iEt^{-i}\lhd G$. 容易看出 $N=C_G(t)\bigcap E$. (事实上, 一方面由定义直接看出 $C_G(t)\bigcap E\subseteq\bigcap\limits_{0\leqslant i\leqslant 2}t^iEt^{-i}=N$. 另一方面, $\forall n\in N$, 有 $n=tet^{-1}$, $e\in E$. 因 $T\lhd G$, 故 $ntn^{-1}\in T$. 但 $ntn^{-1}\neq t^2$, 否则 $t^2n=nt=te$,　$tn=e$, 从而 $t\in T\bigcap E=\{1\}$, 矛盾. 于是 $ntn^{-1}=t$, 即 $nt=tn$. 这表明 $n\in C_G(t)\bigcap E$, 即 $N\subseteq C_G(t)\bigcap E$.)

因 t 只有两个共轭元, 即 t 和 t^2, 故 $C_G(t)=12$. 从而 $|N|$ 是 12 和 $8=|E|$ 的公因子, 即 $|N|=1$, 2 或 4. 但 $|N|\neq 4$ (不然, 设 $|N|=4$. 若 $N\bigcap Z(E)=\{1\}$, 则因 $Z(E)$ 不平凡, 故有 $NZ(E)=E$. 因 4 阶群可换, 即 E 是 Abel 群, 即 $Z(E)=E$. 这与 $N\bigcap Z(E)=\{1\}$ 不合. 于是 $N\bigcap Z(E)\neq\{1\}$. 令 $z\neq 1$, $z\in N\bigcap Z(E)$, 则 z 与 t 及 E 中元都可换, 从而 $z\in Z(G)$. 矛盾!), 从而 $|N|=1$ 或 2. 但 G/N 是 S_3 的子群, 从而 24 阶群或 12 阶群是 6 阶群 S_3 的子群. 矛盾!

这就证明了断言, 即 G 有 4 个 Sylow 3- 子群 T_1, T_2, T_3, T_4. 令 $\Sigma=\{T_i|i=1,2,3,4\}$, 考虑 G 在 Σ 上的共轭作用, 则有群同态 $\rho:\ G\longrightarrow S_4$. 令 $K:=\operatorname{Ker}\rho$, 则

$$K=\{g\in G|gT_ig^{-1}=T_i,\ i=1,2,3,4\}=\bigcap_{1\leqslant i\leqslant 4}N_G(T_i)\lhd G.$$

因 $|N_G(T_i)|=6$, 故 $|K|=1,2,3$ 或 6.

但 $|K|\neq 3$ (否则 G 有 3 阶正规子群 K, 与 $N(3)=4$ 不合.).

又 $|K|\neq 6$ (否则 $N_G(T_i)=N_G(T_j)$, $1\leqslant i,j\leqslant 4$. 于是 T_1, T_2 都是 $N_G(T_1)$ 的 Sylow 3- 子群, 从而由 Sylow 定理知, T_1 与 T_2 在 $N_G(T_1)$ 中共轭, 于是 $T_1=T_2$. 矛盾!).

最后, $|K|\neq 2$ (否则 $K=\{1,\ x\}$. 因 $K\lhd G$, 故 $gxg^{-1}=x$, $\forall g\in G$, 即 $x\in Z(G)$. 矛盾!).

因此 $|K|$=1. 于是 $\rho:\ G\longrightarrow S_4$ 是群同构. ■

§9 自由群和群的表现

知识要点:

外直积与内直积的统一; 直积的等价刻画.

当 $(n,m)=1$ 时, 有群同构 $\mathbb{Z}_n\times\mathbb{Z}_m\cong\mathbb{Z}_{nm}$.

自由群与自由 Abel 群的概念; 任一群同构于自由群的商群; 任一有限生成群同构于有限生成自由群的商群; 由此导出用生成元和定义关系表达任一群.

n 次二面体群 D_n 的生成元和定义关系: $D_n=\langle a,b\mid a^n=1=b^2,\ ba=a^{-1}b\rangle$.

四元数群 Q_8 的生成元和定义关系: $Q_8=\langle a,b\mid a^4=1,\ b^2=a^2,\ ba=a^{-1}b\rangle$.

1.9.1. 设 G_i $(1\leqslant i\leqslant n)$ 为群, $N_i\leqslant G_i$, 则

(1) $G_1\times G_2\cong G_2\times G_1$.

(2) $(G_1\times G_2)\times G_3\cong G_1\times(G_2\times G_3)$.

(3) $Z(G_1\times\cdots\times G_n)=Z(G_1)\times\cdots\times Z(G_n)$.

(4) $G_1\times\cdots\times G_n$ 为 Abel 群当且仅当每个 G_i 均为 Abel 群.

(5) $N_1\times\cdots\times N_n\leqslant G_1\times\cdots\times G_n$.

(6) $N_1\times\cdots\times N_n\lhd G_1\times\cdots\times G_n$ 当且仅当对每个 i, $N_i\lhd G_i$.

(7) 当 $N_1\times\cdots\times N_n\lhd G_1\times\cdots\times G_n$ 时, $(G_1\times\cdots\times G_n)/(N_1\times\cdots\times N_n)\cong(G_1/N_1)\times\cdots\times(G_n/N_n)$.

证 均由定义直接验证. ■

1.9.2. 若 $n\geqslant 3$, 试问 $A_n\times\mathbb{Z}_2$ 与 S_n 是否同构?

解 当 $n\geqslant 3$ 时, S_n 无 2 阶正规子群. 故 $A_n\times\mathbb{Z}_2$ 与 S_n 当然不同构. ■

1.9.3. 设 $G=G_1\times\cdots\times G_n$, H 是 G 的子群. 问 H 是否一定形如 $H=H_1\times\cdots\times H_n$, 其中 $H_i\leqslant G_i$?

解 否. 例如, $K_4=\{(1),(12)(34),(13)(24),(14)(23)\}=\{(1),(12)(34)\}\times\{(1),(13)(24)\}$. 但 $\{(1),(14)(23)\}$ 也是 K_4 的子群. ■

1.9.4. 设 $G = G_1 \times G_2$, $H \lhd G$ 且 $H \bigcap G_i = \{1\}$, $i = 1, 2$. 试证 $H \leqslant Z(G)$. 特别地, H 是 Abel 群.

证 因为 $H \lhd G$, $G_i \lhd G$, $H \bigcap G_i = \{1\}$, 故 H 中任一元与 G_i 中任一元可换, 因此 H 中任一元与 G 中任一元可换, 即 $H \leqslant Z(G)$. ■

1.9.5. 令 $G = G_1 \times \cdots \times G_n$, 且对任意 $i \neq j, 1 \leqslant i, j \leqslant n, |G_i|$ 和 $|G_j|$ 互素. 则 G 的任意子群 H 都是它的子群 $H \bigcap G_i$ $(i = 1, \cdots, n)$ 的直积.

证 设 $h \in H$, $h = h_1 \cdots h_n$, $h_i \in G_i, i = 1, 2, \cdots, n$. 因 G_i 中任一元与 $G_j (i \neq j)$ 中任一元可换, 故对任一整数 t, 有 $h^t = h_1^t \cdots h_n^t$. 令 $a = |G_i|$, $b = \prod\limits_{j \neq i} |G_j|$, 则 $h_i^a = 1$, $h_j^b = 1$ $(j \neq i)$. 因 $(a, b) = 1$, 故有整数 l 和 k, 使得 $la + kb = 1$. 故

$$h_i = h_i^{la+kb} = h_i^{kb} = h^{kb} \in H \bigcap G_i, \quad i = 1, \cdots, n.$$

从而

$$H = (H \bigcap G_1) \cdots (H \bigcap G_n) = (H \bigcap G_1) \times \cdots \times (H \bigcap G_n).$$ ■

1.9.6. 设 G 是有限生成的自由 Abel 群, $\operatorname{rank}(G) = r$. 如果 $g_1, \cdots, g_n$ 是 G 的一组生成元, 则 $n \geqslant r$.

证 设 $e_1, \cdots, e_r$ 是 G 的一组基, 则 $g_i = \sum\limits_{j=1}^{r} a_{ij} e_j$, $1 \leqslant i \leqslant n$. 令 $A = (a_{ij}) \in M_{n \times r}(\mathbb{Z})$. 因 $G = \langle g_1, \cdots, g_n \rangle$, 故 $e_i = \sum\limits_{j=1}^{n} b_{ij} g_j$, $1 \leqslant i \leqslant r$. 令 $B = (b_{ij}) \in M_{r \times n}(\mathbb{Z})$. 于是 $BA \in M_{r \times r}(\mathbb{Z})$. 因 $e_1, \cdots, e_r$ 是一组基, 故 $BA = I_r$, I_r 是单位阵. 于是

$$r = \operatorname{rank}(I_r) = \operatorname{rank}(BA) \leqslant \operatorname{rank}(A) \leqslant n.$$ ■

1.9.7. 如果 n 是正奇数, 求证 $D_{2n} \cong D_n \times \mathbb{Z}_2$.

证 回顾 $D_{2n} = \langle \sigma, \ \tau \mid \sigma^{2n} = 1 = \tau^2, \ \tau\sigma = \sigma^{2n-1}\tau \rangle$.

考虑 D_{2n} 的子群 $\langle \sigma^n \rangle$ 和 $\langle \sigma^2, \tau \rangle$. 首先 $\langle \sigma^2, \tau \rangle = \{\sigma^{2i}, \ \sigma^{2i}\tau \mid 0 \leqslant i \leqslant n-1\}$ 含有 $2n$ 个元. 因为 $[D_{2n} : \langle \sigma^2, \tau \rangle] = \dfrac{4n}{2n} = 2$, 故 $\langle \sigma^2, \ \tau \rangle \lhd D_{2n}$, 且 $\langle \sigma^2, \tau \rangle \cong D_n$ (事实上, $\pi(\sigma^2) = a$, $\pi(\tau) = b$ 就给出了 $\langle \sigma^2, \tau \rangle$ 到 $D_n = \langle a, b \mid a^n = 1 = b^2, \ ba = a^{n-1}b \rangle$ 的群同构.).

又 $\langle \sigma^n \rangle \cong \mathbb{Z}_2$, 因为

$$\sigma^i \tau \sigma^n \tau^{-1} \sigma^{-i} = \sigma^i (\tau\sigma\tau^{-1})^n \sigma^{-i} = \sigma^i \sigma^{-n} \sigma^{-i} = \sigma^{-n},$$

故 $\langle\sigma^n\rangle \lhd D_{2n}$.

因为 n 是正奇数, 故 $\langle\sigma^n\rangle \bigcap \langle\sigma^2,\ \tau\rangle = \{1\}$, 即 $\sigma^n \notin \langle\sigma^2,\ \tau\rangle$. 于是

$$|\langle\sigma^2,\ \tau\rangle\langle\sigma^n\rangle| = 4n = |D_{2n}|.$$

故 $D_{2n} \cong D_n \times \mathbb{Z}_2$. ■

1.9.8. 以 $\mathbb{C}^*$ 表示非零复数乘法群, $\mathbb{R}^+$ 为正实数乘法群, $\mathbb{R}$ 为实数加法群, $\mathbb{Z}$ 为整数加法群, 则

$$\mathbb{C}^* \cong \mathbb{R}^+ \times \mathbb{R}/(2\pi\mathbb{Z}).$$

证 首先 $\mathbb{R}^+ \lhd \mathbb{C}^*$. 令 U 是 $\mathbb{C}^*$ 中模长为 1 的复数全体作成的乘法群, 则 $\mathbb{R}/(2\pi\mathbb{Z}) \cong U$ (事实上, $\theta + 2\pi\mathbb{Z} \mapsto \cos\theta + \mathrm{i}\sin\theta,\ 0 \leqslant \theta < 2\pi$ 就给出了 $\mathbb{R}/(2\pi\mathbb{Z})$ 到 U 的一个群同构.). 因任一非零复数可唯一地表达成 $r(\cos\theta + \mathrm{i}\sin\theta)$ 的形式, 其中 $r \in \mathbb{R}^+,\ 0 \leqslant \theta < 2\pi$, 故

$$\mathbb{C}^* \cong \mathbb{R}^+ \times U \cong \mathbb{R}^+ \times \mathbb{R}/(2\pi\mathbb{Z}).$$ ■

1.9.9. 设 $n_1, \cdots, n_r$ 为自然数, 则

(1) $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cong \mathbb{Z}_{n_1 n_2}$ 当且仅当 $(n_1, n_2) = 1$.

(2) 如果 $n_1, \cdots, n_r$ 两两互素, 则 $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \cong \mathbb{Z}_{n_1 \cdots n_2}$.

证 反复使用 (1) 即可得到 (2), 故只要证 (1).

设 $(n_1, n_2) = 1$. 考虑映射 $\pi:\ \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \longrightarrow \mathbb{Z}_{n_1 n_2},\ \ (\overline{s},\ \overline{t}) \mapsto \overline{sn_2 + tn_1}$. 验证这是映射, 单射, 满射和加法群同态 (注意在验证满射时用到: 存在整数 l 和 m, 使得 $ln_1 + mn_2 = 1$. 从而对任一 $a \in \mathbb{Z}$, $a = aln_1 + amn_2$, 于是 $\overline{a} = \pi(\overline{am}, \overline{al})$).

反之, 若 $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cong \mathbb{Z}_{n_1 n_2} = \langle a\rangle$, 因为循环群的固定阶的子群是唯一的, 故 $\mathbb{Z}_{n_1} = \langle a^{n_2}\rangle$, $\mathbb{Z}_{n_2} = \langle a^{n_1}\rangle$. 而 $1 = \langle a^{n_2}\rangle \bigcap \langle a^{n_1}\rangle = \langle a^{[n_1, n_2]}\rangle$, 故 $n_1 n_2 \mid [n_1, n_2]$, 即 $(n_1, n_2) = 1$. ■

1.9.10. 试证 $7 \cdot 11 \cdot 13$ 阶群一定是循环群.

证 设 $|G| = 7 \cdot 11 \cdot 13$, 则 Sylow 7- 子群的个数 $N(7) = 7k + 1$, 其中 k 为某一非负整数, 且 $N(7) \mid (11 \cdot 13)$. 故 $N(7) = 1$, 从而 $\mathbb{Z}_7 \lhd G$. 同理, $\mathbb{Z}_{11} \lhd G$, $\mathbb{Z}_{13} \lhd G$. 于是

$$G = \mathbb{Z}_7\mathbb{Z}_{11}\mathbb{Z}_{13} = \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13} \cong \mathbb{Z}_{7 \cdot 11 \cdot 13}.$$ ■

1.9.11*. 试证 $5 \cdot 7 \cdot 13$ 阶群为循环群.

证 设 $|G| = 5 \cdot 7 \cdot 13$, 则 Sylow 7- 子群的个数 $N(7) = (7k + 1) \mid 5 \cdot 13$, 其中 k 为某一非负整数, 故 $N(7) = 1$. 从而 G 有 7 阶正规子群 $\langle y\rangle \cong \mathbb{Z}_7$. 同理

G 有 13 阶正规子群 $\langle z\rangle \cong \mathbb{Z}_{13}$. (但注意: 此时不能直接断言 $N(5)=1$.) 设 $\langle x\rangle$ 是 G 的 Sylow 5- 子群, 则 $|\langle x\rangle\langle y\rangle|=35$, $|\langle x\rangle\langle z\rangle|=65$, $|\langle y\rangle\langle z\rangle|=91$. 而 35 阶群、65 阶群和 91 阶群均是 Abel 群, 故 x 与 y, x 与 z, y 与 z 均可换. 从而 $G=\langle x\rangle\langle y\rangle\langle z\rangle$ 可换, 即 $\langle x\rangle \lhd G$, 于是 $G=\langle x\rangle\langle y\rangle\langle z\rangle$ 是 Abel 群. 从而 $\langle x\rangle$ 是 G 的正规子群. 于是

$$G=\langle x\rangle\langle y\rangle\langle z\rangle=\mathbb{Z}_5\times\mathbb{Z}_7\times\mathbb{Z}_{13}\cong\mathbb{Z}_{5\cdot 7\cdot 13}. \qquad \blacksquare$$

1.9.12*. 设 G_1 和 G_2 是两个非交换单群, 试证 $G_1\times G_2$ 的非平凡正规子群只有 G_1 和 G_2.

证 设 N 是 $G_1\times G_2$ 的非平凡正规子群.

若 $G_1\bigcap N=G_1$, 即 $G_1\leqslant N$, 则 $N=G_1\times(N\bigcap G_2)$. 但 G_2 是单群且 $N\neq G_1\times G_2$, 故 $N\bigcap G_2=\{1\}$, 从而 $N=G_1$.

下设 $G_1\bigcap N=\{1\}$, 则 G_1 中任一元与 N 中任一元可换.

令

$$H_1=\{g_1\in G_1 \mid 存在\ g_2\in G_2\ 使得\ g_1g_2\in N\}.$$

则 $H_1\lhd G_1$. 于是 $H_1=\{1\}$ 或 G_1.

若 $H_1=\{1\}$, 则 $N\leqslant G_2$, 从而 $N=G_2$.

若 $H_1=G_1$, 则对任一 $x\in G_1$ 和任一 $g_1\in G_1$, 存在 $g_2\in G_2$, 使得 $g_1g_2\in N$, 从而 x 与 g_1g_2 可换. 但 x 与 $g_2\in G_2$ 也可换, 因此 x 与 g_1 可换. 即 G_1 是 Abel 群, 与题设不合. $\blacksquare$

注 由上述证明可知, 上述结论可推广成: 设 G_1 和 G_2 是单群, 且至少有一个非交换, 则 $G_1\times G_2$ 的非平凡正规子群只有 G_1 和 G_2.

1.9.13*. 令 $G=\langle g_1, g_2,\cdots, g_n\rangle$. 如果 G 的子群 A 具有有限指数 m, 则 A 可以由 $2nm$ 个元生成.

证 记 $g_{n+i}={g_i}^{-1}$. 设 $G=Aa_1\bigcup\cdots\bigcup Aa_m$ 是无交并, $a_1=1$. 则对任意的 i 和 j, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant 2n$, 存在唯一的 k, $1\leqslant k\leqslant m$ 和 $b_{ij}\in A$, 使得

$$a_ig_j=b_{ij}a_k.$$

令 B 是由 $2nm$ 个元 b_{ij} 生成的子群, 则 B 是 A 的子群. 因为 $g_j=a_i^{-1}b_{ij}a_k$, 故 G 可由 b_{ij} 和 a_i 生成, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant 2n$, 即 G 由 B 和 $a_1,\cdots,a_m$ 生成.

下证 $G=Ba_1\bigcup\cdots\bigcup Ba_m$ 是 G 关于 B 的右陪集分解.

因为 $Aa_i\bigcap Aa_j=\varnothing$, $i\neq j$, 故 $Ba_i\bigcap Ba_j=\varnothing$, $i\neq j$.

其次要证 G 中任一元属于某一 Ba_i. 因为 $G=\langle g_1,g_2,\cdots,g_n\rangle$, 故 G 中任一元可写成 $g_1, \cdots, g_n, g_{n+1},\cdots, g_{2n}$ 的某种积. 因任一 $g_j=b_{1j}a_k$, 故只要证

形如 $a_s x$ 的元属于某一 Ba_i, 其中 x 是 $g_1, \cdots, g_n, g_{n+1}, \cdots, g_{2n}$ 的某种积, 而这是对的 (因 $a_s g_j = b_{sj} a_k$, 不断地使用此式即知.).

因此 $[G:B]=m$. 而 $[G:B]=[G:A][A:B]=m[A:B]$, 于是 $[A:B]=1$, 即 $A=B$, 即 A 是由 $2nm$ 个元 b_{ij} 生成. ■

1.9.14*. 试证: 定义关系为

$$x_i^2=1,\ i=1,\cdots,n-1,$$

$$x_i x_j = x_j x_i,\quad i \text{ 与 } j \text{ 不相邻 (即 } j<i-1),$$

$$(x_i x_{i+1})^3=1,\ i<n-2\ \ (\text{即 } \ x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1})$$

的 $n-1$ 个元 $x_1,\cdots,x_{n-1}$ 生成的群 G_n 同构于对称群 S_n.

证 设 $\sigma_n=(i,i+1), i=1,\cdots,n-1$, 则 $S_n=\langle\sigma_1,\cdots,\sigma_{n-1}\rangle$ 且 σ_i 满足上述关系. 故有群满同态 $\pi_n: G_n \longrightarrow S_n,\ \ \pi_n(x_i)=\sigma_i,\ \ i=1,\cdots,n-1$. 以下用归纳法证明 π_n 是群同构. 设 π_{n-1} 是群同构.

断言: $G_{n-1}, G_{n-1}x_{n-1}, \cdots, G_{n-1}x_{n-1}x_{n-2}\cdots x_2 x_1$ 是 G_n 关于 G_{n-1} 的全部的两两不同的右陪集.

首先, 这 n 个右陪集两两不等. (否则, 设 $G_{n-1}x$, $G_{n-1}y$ 是上述两个右陪集, $x\neq y$, $G_{n-1}x=G_{n-1}y$. 则 $xy^{-1}\in G_{n-1}$, 于是 $\pi_n(x)(\pi_n(y))^{-1}\in S_{n-1}$. 而在 S_n 中可作具体的计算, 计算结果表明 $\pi_n(x)(\pi_n(y))^{-1}\notin S_{n-1}$. 矛盾!)

其次, 要证上述 n 个右陪集是 G_n 关于 G_{n-1} 的全部右陪集.

设 $G_{n-1}x\neq G_{n-1}$, 令

$$\Omega=\{y\in G_n \mid G_{n-1}y=G_{n-1}x\}.$$

Ω 中任一元可写成 $x_1,\cdots,x_{n-1}$ 的某种乘积. 令 z 是 Ω 中的元, z 表达成 $x_1,\cdots,x_{n-1}$ 的积时长度最短, 则 z 必以 x_{n-1} 开头 (从左至右).

若 $z\neq x_{n-1}$, 则 $z=x_{n-1}x_{n-2}\cdots$. (否则 $z=x_{n-1}x_j\cdots=x_jx_{n-1}\cdots=x_jz'$, 从而 $G_{n-1}z=G_{n-1}z'$. 与 z 的长度最短不合.)

若 $z\neq x_{n-1}x_{n-2}$, 则 $z=x_{n-1}x_{n-2}x_i\cdots$, $x_i\neq x_{n-1}$ (否则 $z=x_{n-1}x_{n-2}x_{n-1}\cdots=x_{n-2}x_{n-1}x_{n-2}\cdots=x_{n-2}z'$, 从而 $G_{n-1}z=G_{n-1}z'$. 与 z 的长度最短不合!); 并且 $x_i=x_{x-3}$ (否则 x_i 又可以提到最前面).

如此继续下去, 最后逐步可得到 $z=x_{n-1}x_{n-2}\cdots x_i$.

这就证明了 G_n 有右陪集分解

$$G_n=G_{n-1}\bigcup G_{n-1}x_{n-1}\bigcup\cdots\bigcup G_{n-1}x_{n-1}x_{n-2}\cdots x_2x_1.$$

从而 $[G_n:G_{n-1}]=n$, $|G_n|=n|G_{n-1}|=n|S_{n-1}|=n!$.

已知 $|S_n| = n!$, $S_n \cong G_n/\operatorname{Ker}\pi_n$. 故 $\operatorname{Ker}\pi_n = \{1\}$, 即 $S_n \cong G_n$. ■

1.9.15*. 试证: 对 $n \geqslant 3$, 定义关系为

$$x_1^3 = 1,$$

$$x_i^2 = 1,\ i = 2, \cdots, n-2,$$

$$(x_i x_{i+1})^3 = 1,\ i = 1, \cdots, n-3,$$

$$(x_i x_j)^2 = 1,\ i = 1, \cdots, n-4,\ j > i+1$$

的 $n-2$ 个元 $x_1, \cdots, x_{n-2}$ 生成的群 G_n 同构于交错群 A_n.

证　设 $\sigma_1 = (123)$, $\sigma_i = (12)(i+1, i+2)$, $i = 2, \cdots, n-2$, 则 $A_n = \langle \sigma_1, \cdots, \sigma_{n-2} \rangle$ 且满足上述关系. 故有群满同态 $\pi_n : G_n \longrightarrow A_n$, $\pi_n(x_i) = \sigma_i$, $i = 1, \cdots, n-1$. 用归纳法可证 π_n 是群同构.

关键要证 G_{n-1}, $G_{n-1}x_{n-1}, \cdots$, $G_{n-1}x_{n-1}x_{n-2}\cdots x_2x_1, G_{n-1}x_{n-1}x_{n-2}\cdots x_2x_1^2$ 是 G_n 关于 G_{n-1} 的全部的两两不同的右陪集. 这与题 1.9.14 相类似, 不再赘述! ■

§10　有限生成 Abel 群

知识要点:

有限生成自由 Abel 群由秩唯一确定; 有限生成自由 Abel 群的子群仍是有限生成自由 Abel 群.

有限生成 Abel 群是有限生成自由 Abel 群与有限 Abel 群的直和.

有限 Abel 群是其 Sylow 子群的直积. 阶为 p^n 的 Abel 群的同构类与 n 的划分之间的一一对应关系. 会用初等因子和不变因子对有限 Abel 群分类; 诸如求互不同构的 1500 阶 Abel 群.

有限 Abel 群的 Lagrange 定理之逆成立.

1.10.1. 用不变因子的方式写出所有互不同构的 360 阶 Abel 群.

解　用 $p(n)$ 表示 n 的划分的个数.

$360 = 2^3 \times 3^2 \times 5^1$, 故共有 $p(3)p(2)p(1) = 6$ 个互不同构的 360 阶 Abel 群.

我们写出 $3, 2, 1$ 的全部划分:

$$3,\quad 2+1,\quad 1+1+1;$$

$$2,\quad 1+1;$$

$$1.$$

则 6 个互不同构的 360 阶 Abel 群为

$$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{5^1} \cong \mathbb{Z}_{360},$$

$$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{5^1} \cong \mathbb{Z}_{120} \oplus \mathbb{Z}_3,$$

$$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{5^1} \cong \mathbb{Z}_{180} \oplus \mathbb{Z}_2,$$

$$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{5^1} \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_6,$$

$$\mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{5^1} \cong \mathbb{Z}_{90} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,$$

$$\mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{5^1} \cong \mathbb{Z}_{30} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2. \qquad \blacksquare$$

1.10.2. 试证有限生成 Abel 群 G 是有限群当且仅当 G 的一组生成元均是有限阶元.

证　只证充分性. 设 $g_1, \cdots, g_n$ 是 Abel 群 G 的一组生成元, 且 $o(g_i) = m_i < \infty, i = 1, 2, \cdots, n$. 则 $G = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_n$. 令 $F = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n$ 是 n 秩自由 Abel 群, $\pi:\ F \longrightarrow G$ 是由 $\pi(x_i) = g_i,\ \forall\ i = 1, 2, \cdots, n$ 给出的群满同态. 则由题设知 $\operatorname{Ker}\pi \supseteq m_1\mathbb{Z}x_1 \oplus \cdots \oplus m_n\mathbb{Z}x_n$. 因此 π 诱导出群满同态

$$\mathbb{Z}_1 \oplus \cdots \oplus \mathbb{Z}_n \cong \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n / m_1\mathbb{Z}x_1 \oplus \cdots \oplus m_n\mathbb{Z}x_n \to G,$$

故 G 是有限群. $\blacksquare$

1.10.3*. 试证有限生成 Abel 群 G 是自由 Abel 群当且仅当 G 的每个非零元都是无限阶元.

证　必要性由定义直接得出.

设 G 是有限生成 Abel 群且任一非零元的阶为无穷. 设 $G = \langle g_1, \cdots, g_n \rangle$, $g_i \neq 0,\ \forall i = 1, \cdots, n$. 则 $G = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_n$. 不妨设 $\{g_1, \cdots, g_m\}$ 是 $\{g_1, \cdots, g_n\}$ 的一个极大 $\mathbb{Z}$- 线性无关组 (由题设, 这总是存在的, 且不妨设为前 m 个, $m \leqslant n$.). 于是对于任一 $g_{m+i},\ 1 \leqslant i \leqslant n - m$, 存在 $0 \neq \lambda_i \in \mathbb{Z}$, 使得

$$\lambda_i g_{m+i} \in \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_m = \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_m.$$

令 $\lambda = \lambda_1 \cdots \lambda_{n-m} \in \mathbb{Z}$, 则

$$\lambda G \leqslant \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_m.$$

但 $\mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_m$ 是有限生成自由 Abel 群, 故 λG 亦是有限生成自由 Abel 群. 令 $\pi:\ G \longrightarrow \lambda G,\ \ \pi(g) = \lambda g,\ \forall g \in G$. 由题设知 $\operatorname{Ker}\pi = 0$. 即 $G \cong \lambda G$, 故 G 是自由群. $\blacksquare$

1.10.4*. 设 $\mathbb{Q}^+$ 是正有理数乘法群, 试证:

(1) $\mathbb{Q}^+$ 是自由 Abel 群, $\{p \mid p$ 是素数$\}$ 是它的一组基.

(2) $\mathbb{Q}^+$ 不是有限生成的.

证 (1) 任一正有理数形如

$$\frac{q_1^{s_1}\cdots q_m^{s_m}}{p_1^{r_1}\cdots p_n^{r_n}} = \left(\frac{1}{p_1}\right)^{r_1}\cdots\left(\frac{1}{p_n}\right)^{r_n} q_1^{s_1}\cdots q_m^{s_m},$$

其中 $p_1,\cdots,p_n,\ q_1,\cdots,q_m$ 是两两不同的素数. 由算术基本定理知, 这样的表达是唯一的. 由定义知, $\mathbb{Q}^+$ 是秩为无限的自由 Abel 群, $\{p \mid p$ 是素数$\}$ 是它的一组基.

(2) 对于任意有限个 (既约的) 有理数, 其分子、分母中所有的素因子是有限多个. 而熟知, 素数有无穷多个. 故不在这有限个素数之中的素数, 当然不能写成这有限个有理数的某种积, 故 $\mathbb{Q}^+$ 不是有限生成的. ■

1.10.5*. 设 $\mathbb{Q}$ 是有理数加法群, 试证:

(1) $\mathbb{Q}$ 不是自由 Abel 群.

(2) $\mathbb{Q}$ 的任意有限生成的子群都是循环群, 但 $\mathbb{Q}$ 不是循环群.

证 (1) 假设 $(\mathbb{Q},+)$ 是自由 Abel 群, $\left\{\dfrac{b_i}{a_i} \mid i\in J\right\}$ 是其一组基, 其中 a_i, b_i 均为正整数, J 为指标集, 即对任一有理数 r, 存在唯一的 J 的有限子集 I 和唯一的一组整数 r_i, $i\in I$, 使得

$$r=\sum_{i\in I} r_i\frac{b_i}{a_i}.$$

则 $\left\{\dfrac{1}{a_i} \mid i\in J\right\}$ 也是其一组基. 因为 $1=a_i\cdot\dfrac{1}{a_i}$, $\forall i\in J$, 故 J 只能含有一个元, 即 $(\mathbb{Q},+)$ 是循环群, 即 $\mathbb{Q}=\left\langle\dfrac{1}{a}\right\rangle$. 这很荒唐: 因为存在无穷多个素数, 故可设素数 p 不是 a 的因子, 则 $\dfrac{1}{p}$ 不是 $\dfrac{1}{a}$ 的整数倍!

(2) 设 $H=\left\langle\dfrac{b_1}{a_1},\cdots,\dfrac{b_n}{a_n}\right\rangle$ 是 $\mathbb{Q}$ 的有限生成子群, 则 $H=\left\langle\dfrac{1}{a_1},\cdots,\dfrac{1}{a_n}\right\rangle$, 其中 $a_1,\cdots,a_n$ 均为正整数. 令 $[a_1,\cdots,a_n]$ 是 $a_1,\cdots,a_n$ 的最小公倍数, 则有正整数 m_i, 使得 $a_im_i=[a_1,\cdots,a_n]i=1,\cdots,n$. 于是

$$\frac{1}{a_i}=\frac{m_i}{[a_1,\cdots,a_n]},\ 1\leqslant i\leqslant n,$$

这表明

$$H=\left\langle\frac{1}{[a_1,\cdots,a_n]}\right\rangle.$$

$\Big($事实上, $(m_1, \cdots, m_n) = 1$, 故存在整数 $c_1, \cdots, c_n$, 使得 $\sum\limits_{i=1}^{n} m_i c_i = 1$. 从而 $\dfrac{1}{[a_1, \cdots, a_n]} = \sum\limits_{i=1}^{n} \dfrac{c_i}{a_i} \in H.\Big)$ ■

1.10.6. 设 A 为有限 Abel 群, 则对于 $|A|$ 的每个正因子 d, A 均有 d 阶子群和 d 阶商群.

证 只要证 A 有 d 阶子群. 因为 A 是其 Sylow 子群的直和, 故只要对 Abel p- 群 A 证明此结论.

设 $|A| = p^n$, 则 $d = p^m$, $m \leqslant n$. 设 $A = A_1 \oplus \cdots \oplus A_t$, 其中 A_i 均为循环 p-群. 对 t 用归纳法. $t = 1$ 时, A 为循环群, 故结论正确. 若 $|A_1| \cdots |A_{t-1}| \geqslant p^m$, 则由归纳假设 $A_1 \oplus \cdots \oplus A_{t-1}$ 有 d 阶子群. 若 $|A_1| \cdots |A_{t-1}| < p^m$, 设 $|A_t| = p^l$, 则 A_t 有 p^{l+m-n} 阶子群 H, 于是 $A_1 \oplus \cdots \oplus A_{t-1} \oplus H$ 即为 A 的 d 阶子群. ■

1.10.7. 设 H 是有限 Abel 群 A 的子群, 则有 A 的子群同构于 A/H.

证 设 $A = G_1 \oplus \cdots \oplus G_m$, 其中 G_i 是 A 的 Sylow p- 子群 $i = 1, \cdots, m$. 则由题 1.9.5 知

$$H = H_1 \oplus \cdots \oplus H_m, \quad H_i = H \bigcap G_i, \quad 1 \leqslant i \leqslant m.$$

因为

$$A/H \cong G_1/H_1 \oplus \cdots \oplus G_m/H_m,$$

故只要证明 G_i 有子群与 G_i/H_i 同构即可. 即不妨设 $|A| = p^n$, $n \geqslant 1$, $|H| = p^m$, $m \leqslant n$.

由 Abel p- 群的结构知

$$A = \mathbb{Z}_{p^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_t}}, \quad H = \mathbb{Z}_{p^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{s_t}},$$

其中 $\mathbb{Z}_{p^{s_i}} \leqslant \mathbb{Z}_{p^{r_i}}$, $1 \leqslant i \leqslant t$, $r_1 + \cdots + r_t = n$, $s_1 + \cdots + s_t = m$, r_i 均为正整数, s_i 均为非负整数, 且 $s_i \leqslant r_i$. 因此

$$A/H \cong \mathbb{Z}_{p^{r_1 - s_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_t - s_t}} \leqslant A.$$ ■

1.10.8. 如果有限 Abel 群 A 不是循环群, 则存在素数 p 使得 A 有子群同构于 $\mathbb{Z}_p^2 = \mathbb{Z}_p \oplus \mathbb{Z}_p$.

证 若 A 不是循环群, 则存在素数 p 使得 A 的 Sylow p- 子群 A_p 不是循环群. 而 A_p 是循环 p- 群的直和, 故 A_p 有形如 $\mathbb{Z}_p \oplus \mathbb{Z}_p$ 的子群. ■

1.10.9. 试证: 当 $(m,n)=1$ 时, $\mathbb{Z}_m\oplus\mathbb{Z}_n$ 的不变因子组为 $\{mn\}$; 而当 $(m,n)>1$ 时, $\mathbb{Z}_m\oplus\mathbb{Z}_n$ 的不变因子组为 $\{(m,n),[m,n]\}$.

证 当 $(m,n)=1$ 时, $\mathbb{Z}_m\oplus\mathbb{Z}_n\cong\mathbb{Z}_{mn}$, 故其不变因子组为 $\{mn\}$.

当 $(m,n)>1$ 时, 设 $m=p_1^{t_1}\cdots p_l^{t_l}$, $n=p_1^{s_1}\cdots p_l^{s_l}$, 这里 $p_1,\cdots,p_l$ 是互不相同的素数, $t_1,\cdots,t_l$, $s_1,\cdots,s_l$ 是非负整数, 但对每一 i, t_i 与 s_i 不同时为 0. 于是

$$\mathbb{Z}_m=\mathbb{Z}_{p_1^{t_1}}\oplus\cdots\oplus\mathbb{Z}_{p_l^{t_l}},\quad \mathbb{Z}_n=\mathbb{Z}_{p_1^{s_1}}\oplus\cdots\oplus\mathbb{Z}_{p_l^{s_l}}.$$

从而 $\mathbb{Z}_m\oplus\mathbb{Z}_n$ 的初等因子组是从

$$(p_1^{t_1},\ p_1^{s_1},\ \cdots,\ p_l^{t_l},\ p_l^{s_l})$$

中删去为 1 的因子后得到的数组. 从而其不变因子为

$$\prod_{i=1}^{l}p_i^{\min(t_i,s_i)},\ \prod_{i=1}^{l}p_i^{\max(t_i,s_i)}.$$

前者恰为 $(m,n)>1$, 后者恰为 $[m,n]$, 故不变因子组为 $\{(m,n),\ [m,n]\}$. ■

1.10.10. 求 $\mathbb{Z}_2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{35}$ 的初等因子组和不变因子组.

解 $\mathbb{Z}_2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{35}=\mathbb{Z}_2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_5\oplus\mathbb{Z}_7=\mathbb{Z}_{630}$, 因此其初等因子组为 $(2,3^2,5,7)$, 而其不变因子组为 $\{630\}$. ■

1.10.11. 试证非零复数乘法群 $\mathbb{C}^*$ 的每个有限子群都是循环群.

解 设 G 是 $\mathbb{C}^*$ 的 n 阶子群, 则 G 恰是方程 $x^n=1$ 在复数域 $\mathbb{C}$ 中的解集, 故 G 是循环群. ■

1.10.12. 设 G, A, B 均为有限 Abel 群. 如果 $G\oplus A\cong G\oplus B$, 求证 $A\cong B$.

证 $G\oplus A$ 的初等因子组是 G 的初等因子组与 A 的初等因子组的合并, 而 $G\oplus A$ 与 $G\oplus B$ 有相同的初等因子组, 故 A 与 B 有相同的初等因子组, 从而 A 与 B 同构. ■

1.10.13*. 设 p 是一个素数, $\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$ 有多少个 p^2 阶子群?

解 方便起见, 将 G 的运算写成乘法. 令 $G=\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}=\langle x\rangle\langle y\rangle$, $o(x)=p^3$, $o(y)=p^2$.

I. 计算 G 中 p 阶元的个数.

设 x^iy^j 是 G 中 p 阶元, 则 x^i 和 y^j 均为 p 阶元. 因此 $i=kp^2$, $j=k'p$, $k,\ k'=0,\cdots,p-1$, $(i,j)\neq(0,0)$. 于是共有 p^2-1 个 p 阶元.

II. 计算 G 中形如 $\mathbb{Z}_p\oplus\mathbb{Z}_p$ 的 p^2 阶子群 H 的个数.

设 $H \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, $H \leqslant G$. 则 H 中有 p^2-1 个 p 阶元. 因此, H 恰是 G 中所有 p 阶元再加上 1 得到的集合. 故 G 只有唯一的 p^2 阶子群同构于 $\mathbb{Z}_p \oplus \mathbb{Z}_p$, 剩下的 p^2 阶子群必是循环群.

Ⅲ. 计算 G 中 p^2 阶元的个数.

易知 G 中 p^3 阶元的全体为 x^iy^j, 其中 $0 \leqslant j \leqslant p^2-1$, x^i 是 p^3 阶元, 故 i 与 p 互素, 即 $i = kp+t$, $k=0,\cdots,p^2-1$, $t=1,\cdots,p-1$. 即 G 有 $p^2p^2(p-1)=p^4(p-1)$ 个 p^3 阶元. 故 G 中 p^2 阶元的个数为

$$p^5-p^4(p-1)-(p^2-1)-1=p^4-p^2=p^2(p^2-1).$$

IV. 计算 G 中 p^2 阶循环子群的个数.

每个 p^2 阶循环子群中有 $p(p-1)$ 个 p^2 阶元. 不同的 p^2 阶循环子群不可能有相同的 p^2 阶元. 故 G 共有

$$\frac{p^2(p^2-1)}{p(p-1)}=p(p+1)$$

个 p^2 阶循环子群.

综上所述, G 有 $p(p+1)+1=p^2+p+1$ 个 p^2 阶子群. ■

1.10.14*. 设 G 是 n 个 p 阶群的直和, 问 G 有多少个极大子群?

解 记 $G=G_n$, t_n 是 G_n 中极大子群的个数.

I. 对任一 $a\neq 1$, $b\neq 1$, a, $b\in G$, 存在 G 的自同构 π 使 $\pi(a)=b$.

事实上, 存在 $H, L\leqslant G$, 使得 $\langle a\rangle\oplus H=G=\langle b\rangle\oplus L$. 因为 $H\cong L\cong G_{n-1}$, 故存在群同构 $\pi': H\longrightarrow L$. 则 $\pi: G\longrightarrow G$, $\pi|_H=\pi'$, $\pi(a)=b$ 给出所需的自同构.

Ⅱ. 对任一 $a\neq 1$, $a\in G$, 记 $s_n(a)$ 为 G_n 的包含 a 的极大子群的个数. 则 $s_n(a)$ 不依赖于 a, 即 $s_n(a)=s_n(b)$, $\forall\, 1\neq b\in G_n$.

事实上, 设 $H_1,\cdots,H_{s_n(a)}$ 是 G 的包含 a 的极大子群的全体, 则 $\pi(H_1),\cdots,\pi(H_{s_n(a)})$ 就是 G 的包含 b 的极大子群的全体, 其中 π 是将 a 送到 b 的 G 的一个自同构.

以下记 $s_n(a)=s_n$.

Ⅲ. 我们有 $(p^{n-1}-1)t_n=(p^n-1)s_n$.

事实上, 令 $\mathcal{M}$ 是 G_n 的极大子群的集合, 令

$$\Omega=\{(H,a)\in\mathcal{M}\times G \mid H+\langle a\rangle=H\}.$$

先固定极大子群 H 得到

$$|\Omega|=\sum_{H\in\mathcal{M}}p^{n-1}=p^{n-1}t_n.$$

先固定元 a, 计算极大子群 H 的个数, 其中 $H+\langle a\rangle = H$. 这个个数恰是 s_n, 如果 $a\neq 1$. 因此

$$|\Omega| = t_n + \sum_{a\neq 1, a\in G} s_n = (p^n-1)s_n + t_n.$$

由此即得.

IV. 我们有 $s_n = t_{n-1}$.

事实上, 令 $H_1,\cdots,H_s$ 是 G 中包含固定元 a 的全体 (两两不同的) 极大子群, 这里 $a\neq 1$, $s=s_n$. 将 G 写成

$$G = \langle a\rangle \oplus \langle x_1\rangle \oplus\cdots\oplus \langle x_{n-1}\rangle,$$

将 H_i 写成 $H_i = \langle a\rangle \oplus L_i$, $1\leqslant i\leqslant s$, 其中 L_i 是 $G_{n-1} = \langle x_1\rangle\oplus\cdots\oplus\langle x_{n-1}\rangle$ 的子群. 因为 G_n 的子群 H 是极大子群当且仅当 $|H| = p^{n-1}$. 故 L_i 均是 G_{n-1} 的极大子群, $1\leqslant i\leqslant s$.

对 G_{n-1} 的任一极大子群 L, $\langle a\rangle\oplus L$ 是 G_n 的含 a 的极大子群. 设 L, L' 是 G_{n-1} 的两个不同的极大子群, 则

$$\langle a\rangle \oplus L \neq \langle a\rangle\oplus L'.$$

(否则, 设 $y\in L', y\notin L$, 则 $y = ka + x$, $x\in L$, $ka\neq 0$. 但 $G = \langle a\rangle\oplus\langle x_1\rangle\oplus\cdots\oplus\langle x_{n-1}\rangle$, L, $L'\leqslant \langle x_1\rangle\oplus\cdots\oplus\langle x_{n-1}\rangle$, 于是得到 $0\neq ka\in\langle a\rangle\bigcap(\langle x_1\rangle\oplus\cdots\oplus\langle x_{n-1}\rangle)$. 矛盾!)

因此, $\langle a\rangle\oplus L$ 是 G 中包含 a 的全体 (两两不同的) 极大子群, 其中 L 是 G_{n-1} 的全体 (两两不同的) 极大子群. 从而得到 $s_n = t_{n-1}$.

综上所述, 我们有递归公式

$$t_n = \frac{p^n-1}{p^{n-1}-1}t_{n-1}.$$

从而

$$t_n = \frac{p^n-1}{p-1},$$

即 G 的极大子群的个数为 $\dfrac{p^n-1}{p-1}$. ■

注 (1) 学过有限域后, 此题可归结为 p 元域上 n 维线性空间中 $n-1$ 维子空间的个数.

(2) 上述证明也得到: 若 G 是 n 个 p 阶群的直和, $a\neq 1$, $a\in G$, 则 G 有 $\dfrac{p^{n-1}-1}{p-1}$ 个极大子群包含 a.

1.10.15*. 如果有限群 G 的每个极大子群都是单群且都在 G 中正规, 则 G 只能是 p 阶群, 或 p^2 阶群, 或 pq 阶循环群, p, q 是不同的素数.

证 情形 I. 设 G 至少有两个不同的极大子群 M_1, M_2, 则由题设 $M_1 \bigcap M_2 \lhd G$. 故 $M_1 \bigcap M_2$ 是 M_i 的正规子群, $i=1,2$. 但 M_i 是单群且 $M_1 \neq M_2$, 故 $M_1 \bigcap M_2 = \{1\}$. 从而 $G = M_1 \times M_2$. 因 M_1 极大, 故 $G/M_1 \cong M_2$ 除了 $\{1\}$ 和 M_2 自身外无其他子群. 因此 M_2 只能是素数阶群, 同理 M_1 只能是素数阶群. 因此 $|G| = pq$, p, q 是素数. 于是 G 是 p^2 阶群, 或

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}, \quad p \neq q,$$

即 G 是 pq 阶群.

情形 II. 设 G 有唯一的极大子群 M, 则 G 是循环 p- 群 (参见题 1.4.6). 设 $|G| = p^n$, $n \geqslant 1$. 若 $n \geqslant 3$, 则 G 的极大子群 M 的阶为 p^{n-1}, $n-1 \geqslant 2$, 从而 M 非单. 这与题设不合. 因此 $|G| = p$ 或 p^2.

综上所述, G 只能是 p 阶群, 或 p^2 阶群, 或 pq 阶循环群. ■

1.10.16*. 设 $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$, p 是素数, 则 G 有 p 阶自同构.

证 为方便起见, 将 G 的运算写成乘法, 设 $G = \langle x \rangle \langle y \rangle$. 对任一数组 $(i,j) \neq (0,0)$, $0 \leqslant i,j \leqslant p-1$, 取任一数组 (s,t), $0 \leqslant s,t \leqslant p-1$, 使得 $(s,t) \neq m(i,j)$, $m = 0, \cdots, p-1$. 则

$$\pi(x) = x^i y^j, \quad \pi(y) = x^s y^t$$

给出 G 的一个自同构. 对于固定的非零数组 (i,j), 非零数组 (s,t) 有 $(p^2 - p) = p(p-1)$ 种不同的取法. 因此 G 共有 $(p^2-1)p(p-1)$ 个自同构. 即 $|\operatorname{Aut}(G)| = p(p-1)^2(p+1)$, 故由 Sylow 定理知, 群 $\operatorname{Aut}(G)$ 有 p 阶元, 即 G 有 p 阶自同构. ■

1.10.17*. 设 $|G| = p^a q^b$, p, q 是不同的素数. 若群 G 没有 p 阶自同构, 则 $a = 0$ 或 1.

证 设 $a \neq 0$. 令 $I(G)$ 是 G 的内自同构群, 则熟知

$$G/Z(G) \cong I(G).$$

由题设 $I(G)$ 中无 p 阶元, 故 $G/Z(G)$ 中无 p 阶元. 因此 p 不是 $G/Z(G)$ 的因子.

令 P 是 G 的 Sylow p- 子群, 则

$$(PZ(G))/Z(G) \cong P/(P \bigcap Z(G)) \leqslant G/Z(G).$$

因此 $P = P \bigcap Z(G)$, 即 $P \leqslant Z(G)$, 于是 $P \lhd G$. 令 Q 是 G 的 Sylow q- 子群, 于是 $|PQ| = p^a q^b$, 故 $G = PQ$. 因 $P \leqslant Z(G)$, 故 $Q \lhd G$, 从而 $G = P \times Q$. 因 P 是 Abel 群, $|P| = p^a$.

下证 $a = 1$. 否则 $a \geqslant 2$. 因 G 没有 p 阶自同构, 由题 1.10.16 可推知 P 无直积因子 $\mathbb{Z}_p \oplus \mathbb{Z}_p$, 因此 P 必有直积因子 $\mathbb{Z}_{p^n}$, $n \geqslant 2$, 则 $G = \mathbb{Z}_{p^n} \times H$. 令 $\mathbb{Z}_{p^n} = \langle x \rangle$, 并令 $\pi : G \longrightarrow G$, $\pi|_H = \mathrm{id}$, $\pi(x) = x^{p^{n-1}+1}$, 则 $1 \neq \pi$ 给出 G 的自同构且 π 是 p 阶元, 矛盾! ■

§11　小阶群的结构

知识要点:

$2p$ 阶非 Abel 群 (p 为素数) 同构于 p 次二面体群 D_p.

设 p, q 均为素数, $p > q$, $q \nmid p-1$, 则 pq 阶群同构于循环群 $\mathbb{Z}_{pq}$.

8 阶非 Abel 群的分类: 四次二面体群 $D_4 = \langle a, b \mid a^4 = 1 = b^2,\ ba = a^{-1}b \rangle$ 和四元数群 $Q_8 = \langle a, b \mid a^4 = 1,\ b^2 = a^2,\ ba = a^{-1}b \rangle$.

12 阶非 Abel 群的分类: 交错群 A_4, 六次二面体群 $D_6 = \langle a, b \mid a^6 = 1 = b^2,\ ba = a^{-1}b \rangle$ 和群 $\langle a, b \mid a^6 = 1,\ b^2 = a^3,\ ba = a^{-1}b \rangle$.

1 至 15 阶群的确定.

1.11.1. 求 D_4 和 Q_8 的中心 $Z(D_4)$ 和 $Z(Q_8)$.

解　设 G 是 8 阶非 Abel 群. 则 $Z(G) \neq 1$ (因为 p 群的中心非平凡), 且 $|Z(G)| \neq 4$ (否则 $G/Z(G)$ 是循环群, 从而 G 是 Abel 群), 因此 $|Z(G)| = 2$.

对于

$$D_4 = \langle a, b | a^4 = 1 = b^2, ba = a^3 b \rangle$$

和

$$Q_8 = \langle a, b | a^4 = 1, b^2 = a^2, ba = a^3 b \rangle$$

均有

$$ba^2 = a^3 ba = a^3 a^3 b = a^2 b.$$

故 $Z(D_4) = \{1, a^2\}$,　$Z(Q_8) = \{1, a^2\}$. ■

1.11.2. 每一子群都是正规子群的群称为 Hamilton 群. 试证 Q_8 是 (非交换的) Hamilton 群.

证　Q_8 只有一个 2 阶元 a^2, 故 2 元子群必是 $\langle a^2 \rangle$ 且正规.

而 Q_8 的 4 阶子群指数是 2, 当然正规. 因此 Q_8 的任一子群均正规. ■

1.11.3. 设 $|G| = p^n$, $n \geqslant 1$, 则阶为 p^{n-1} 的子群 H 一定是正规的.

证　对 n 用归纳法.

若 $Z(G) \nsubseteq H$, 则 $Z(G) \cdot H = G$. 于是易证 $gHG^{-1} = H, \forall g \in G$, 即 $H \lhd G$.

若 $Z(G) \subseteq H$, 则 $H/Z(G) \leqslant G/Z(G)$, 而 $|G/Z(G)| < p^n$ (p 群有非平凡的中心), 故由归纳假设知 $H/Z(G) \lhd G/Z(G)$, 从而 $H \lhd G$. ■

1.11.4*. 确定所有互不同构的 18 阶群.

解 设 $|G| = 18 = 2 \cdot 3^2$, 故 18 阶 Abel 群为 $\mathbb{Z}_{18}$ 和 $\mathbb{Z}_6 \oplus \mathbb{Z}_3$. 下面确定 18 阶非 Abel 群.

G 的 Sylow 3- 子群 H 的指数为 2, 故是正规子群.

若 $H = \langle a \rangle$, $a^9 = 1$, 取 2 阶元 b, 则 $G = \langle a, b \rangle$. 设 $bab^{-1} = a^r$, 则 $r^2 \equiv 1 \pmod 9$, 因此 $r = 8$. 即

$$bab^{-1} = a^8.$$

因此 $G \cong D_9 = \langle a, b \mid a^9 = 1 = b^2,\ ba = a^8 b \rangle$.

下设 $H = \langle a \rangle \times \langle b \rangle$, a 与 b 的阶均为 3. 取 2 阶元 c, 则 $G = \langle a, b, c \rangle$. 令 $cac^{-1} = a^i b^j$, $cbc^{-1} = a^s b^t$. 因为

$$a = c^2 a c^{-2} = c a^i b^j c^{-1} = (a^i b^j)^i (a^s b^t)^j = a^{i^2 + sj} b^{ij + tj},$$

故

$$i^2 + sj \equiv 1, \quad j(i + t) \equiv 0 \pmod 3.$$

同理

$$t^2 + sj \equiv 1, \quad s(i + t) \equiv 0 \pmod 3.$$

首先, 若 $s = 0$, 即 $cac^{-1} = a^i b^j$, $cbc^{-1} = b^t$, 则

$$cbc^{-1} = b^t, \quad cac^{-1} = b^j a^i.$$

因此这转化成 $j = 0$ 的情形 (将上式中 b 记为 a, a 记成 b). 故以下不考虑 $s = 0$ 的情形, 除非 j 同时也为 0.

情形 I. 当 $j = s = 0$, 有 $i^2 \equiv 1 \equiv t^2 \pmod 3$. 因此

$$(i, t) = (1, 1), \text{ 或 } (1, 2), \text{ 或 } (2, 1), \text{ 或 } (2, 2).$$

因 G 非 Abel 群, 故 $(i, t) \neq (1, 1)$.

(1) 设 $(i, t) = (1, 2)$, 则得到

$$cac^{-1} = a, \quad cbc^{-1} = b^2.$$

(2) 设 $(i, t) = (2, 1)$, 则得到

$$cac^{-1} = a^2, \quad cbc^{-1} = b.$$

如将 b 记成 a, a 记成 b, 这就转化成 (1).

(3) 设 $(i,t)=(2,2)$, 则得到

$$cac^{-1}=a^2,\quad cbc^{-1}=b^2.$$

情形 Ⅱ. 当 $s\neq 0, j=0$ 时, $i+t\equiv 0$, $i^2\equiv 1\equiv t^2 \pmod 3$. 于是

$$(i,t)=(1,2),\ 或\ (2,1).$$

(1) 设 $(i,t)=(1,2)$, 则

$$cac^{-1}=a,\quad cbc^{-1}=a^sb^2,\quad s\neq 0.$$

因 $s\neq 0$, 故 $s^2\equiv 1 \pmod 3$. 于是

$$cab^sc^{-1}=a(a^sb^2)^s=a^{s^2+1}b^{2s}=a^2b^{2s}=(ab^s)^2.$$

因 $s\neq 0$, 故可将 ab^s 记成 b. 则转化成情形 I 中 (1).

(2) 设 $(i,t)=(2,1)$, 则

$$cac^{-1}=a^2,\quad cbc^{-1}=a^sb.$$

将 $a^{-s}b$ 记成 a, a 记成 b, 则又转化成情形 I 中的 (1).

于是情形 Ⅱ 均转化成情形 I 中的 (1).

情形 Ⅲ. 设 $s\neq 0$, $j\neq 0$.

(1) 若 $j=1$, 则 $i+t\equiv 0$, $i^2+s\equiv 1\equiv t^2+s \pmod 3$.

若 $(i,t)\neq(0,0)$, 则 $(i,t)=(1,2)$ 或 $(2,1)$. 于是 $i^2\equiv 1\equiv t^2$, 从而 $s=0$, 矛盾! 因此 $i=t=0$. 此时 $s=1$, 即

$$cac^{-1}=b,\quad cbc^{-1}=a.$$

这又转化成情形 I 中的 (1) (将 ab 记成 a, 将 ab^2 记成 b).

(2) 若 $j=2$, 则 $i+t\equiv 0$, $i^2+2s\equiv 1\equiv t^2+2s \pmod 3$.

同理 $i=t=0$, 此时 $s=2$. 即

$$cac^{-1}=b^2,\quad cbc^{-1}=a^2.$$

将 ab^2 记成 a, ab 记成 b, 则又归结为情形 I 中的 (1).

综上所述, 当 G 的 Sylow 3- 子群为 $\mathbb{Z}_3\oplus\mathbb{Z}_3$ 时, $G=\langle a,b,c\rangle$, 满足

(i) $a^3=b^3=1,\ c^2=1,\ ab=ba,\ ca=ac,\ cb=b^2c.$

(ii) $a^3=b^3=1,\ c^2=1,\ ab=ba,\ ca=a^2c,\ cb=b^2c.$

这两种情形不同构. 因为在 (i) 中 ac 的阶为 6, 而在 (ii) 中没有 6 阶元. (只要说明 a^ib^jc 的阶不为 6. 事实上,

$$(a^ib^jc)^2 = a^ib^j(ca^ic^{-1})(cb^jc) = a^ib^ja^{2i}b^{2j} = 1.)$$

最后仍需说明定义关系为 (i), (ii) 的群确实是 18 阶群.

令 $T = \mathbb{Z}_3 \times D_3$, 则 T 满足关系 (i), 且 $|T| = 18$.

令 S 是 $S_3 \times S_3$ 中由

$$a = ((123), 1), \quad b = (1, (123)), \quad c = ((12), (12))$$

生成的子群, 则 S 的定义关系恰好为 (ii) 且 $|S| = 18$.

综上所述, 18 阶群共有 5 个:

$$\begin{aligned}
&\mathbb{Z}_{18}, \quad \mathbb{Z}_6 \oplus \mathbb{Z}_3,\\
&D_9 = \langle a, b \mid a^9 = 1 = b^2, ba = a^8b\rangle,\\
&\mathbb{Z}_3 \times D_3 = \langle a, b, c \mid a^3 = b^3 = c^2 = 1, ba = ab, ca = ac, cb = b^2c\rangle,\\
&S = \langle a, b, c \mid a^3 = b^3 = c^2 = 1, ba = ab, ca = a^2c, cb = b^2c\rangle.
\end{aligned}$$

■

1.11.5*. 确定所有互不同构的 20 阶群.

解 因 $20 = 2^2 \cdot 5$, 故 20 阶 Abel 群有两个, 即 $\mathbb{Z}_{20}$ 和 $\mathbb{Z}_{10} \oplus \mathbb{Z}_2$. 下面确定 20 阶非 Abel 群.

由 Sylow 定理知 G 的 Sylow 5- 子群 $\langle a\rangle$ 是正规子群.

情形 I. 设 G 的 Sylow 2- 子群 H 是循环群, 即 $H = \langle b\rangle$, b 的阶为 4, 则 $G = \langle a, b\rangle$. 设 $bab^{-1} = a^i$. 因 G 非 Abel 群, 故 i 只可能为 2,3,4. 于是 $bab^{-1} = a^2$ 或 $bab^{-1} = a^3$ 或 $bab^{-1} = a^4$.

若 $bab^{-1} = a^3$, 则 $G = \langle a, b^3\rangle$, b^3 的阶亦为 4, 且

$$b^3ab^{-3} = ((a^3)^3)^3 = a^{27} = a^2.$$

这就转化为 $i = 2$ 的情况. 因此我们得到 G 由 5 阶元 a 和 4 阶元 b 生成, 满足 $ba = a^2b$, 或 $ba = a^4b$.

为了说明由生成元和定义关系 $\langle a, b \mid a^5 = 1 = b^4, ba = a^2b\rangle$ 给出的群 (它在同构意义下是唯一的) 的确是 20 阶群 (它最多 20 阶), 令 T 是 $S_5 \times \mathbb{Z}_4$ 中由

$$a = ((12345), 1) \quad 和 \quad b = ((2345), \alpha)$$

生成的子群, 则 T 是 20 阶群且满足上述关系. 因此 T 的定义关系就是上述关系.

为了说明由生成元和定义关系 $\langle a,b \mid a^5=1=b^4, ba=a^4b\rangle$ 给出的群 (它在同构意义下是唯一的) 的确是 20 阶群 (它最多 20 阶), 令 S 是 $S_5\times\mathbb{Z}_4$ 中由

$$a=((12345),1) \quad 和 \quad b=((12)(35),\alpha)$$

生成的子群, 则 S 是 20 阶群且满足上述关系. 因此 S 的定义关系就是上述关系.

注意 S 与 T 不同构: 在 S 中有中心元 b^2, 但是 T 无非平凡的中心元 (否则设为 a^ib^j, 则 $a^ib^ja=aa^ib^j$, 即 $b^ja=ab^j$, $b^jab^{-j}=a$, 这推出 $j=0$. 但 $a^i, i\neq 0$ 不是中心元.).

情形 Ⅱ. 设 G 的 Sylow 2- 子群 H 是 $\langle b\rangle\times\langle c\rangle$, 其中 b 与 c 的阶为 2, 则 $G=\langle a,b,c\rangle$.

设 $bab^{-1}=a^i$, 则

$$a=b^2ab^{-2}=a^{i^2},$$

故 $i^2\equiv 1 \pmod 5$. 故 $i=1$ 或 4, 即 $bab^{-1}=a$ 或 $bab^{-1}=a^4$. 同理 $cac^{-1}=a$ 或 $cac^{-1}=a^4$.

因为 G 非 Abel 群, 故只有以下三种情况.

(1)　$bab^{-1}=a,\quad cac^{-1}=a^4.$

(2)　$bab^{-1}=a^4,\quad cac^{-1}=a.$

(3)　$bab^{-1}=a^4,\quad cac^{-1}=a^4.$

显然情况 (2) 化为 (1) (记 b 为 c, c 为 b). 而对于情况 (3) 有

$$bca(bc)^{-1}=bcac^{-1}b^{-1}=ba^4b^{-1}=(bab^{-1})^4=(a^4)^4=a^{16}=a.$$

因此这一情况也转化为情况(1)　(记 bc 为 b, c 为 c).

因此我们得到 G 是由 5 阶元 a 和 2 阶元 b 和 c 生成, 满足

$$bab^{-1}=a, cac^{-1}=a^4.$$

令 $x=ab$, 则 x 的阶为 10, 且 $x^6=a, x^5=b$. 于是 $G=\langle x,c\rangle$ 满足 $x^{10}=1=c^2$, $cxc^{-1}=a^4b=x^9$. 于是

$$G\cong D_{10}=\langle x,c \mid x^{10}=1=c^2, cx=x^9c\rangle = D_5\times\mathbb{Z}_2.$$

注意到 D_{10} 无 4 阶元, 故不同构于 T, 也不同构于 S. 综上所述, 20 阶群有 5 个:

$\mathbb{Z}_{20},\quad \mathbb{Z}_{10}\oplus\mathbb{Z}_2,$

$T=\langle a,b \mid a^5=1=b^4, ba=a^2b\rangle=\langle a,b \mid a^5=1=b^4, ba=a^3b\rangle,$

$S=\langle a,b \mid a^5=1=b^4, ba=a^4b\rangle=\langle a,b \mid a^{10}=1, b^2=a^5, ba=a^9b\rangle,$

$D_{10}=\langle a,b \mid a^{10}=1=b^2, ba=a^9b\rangle\cong D_5\times\mathbb{Z}_2.$ ■

1.11.6*. 设 p, q 是两个素数, $p < q$. 试证: pq 阶非 Abel 群 G 一定可以由下述生成元和定义关系给出:

$$G = \langle a, b \mid a^p = 1 = b^q, a^{-1}ba = b^r \rangle,$$

其中 $r^p \equiv 1 (\mathrm{mod}\ q)$, q 不整除 $r-1$, p 整除 $q-1$.

证 G 的 Sylow q- 子群的个数 $N(q) = kq + 1$ 且 $N(q)|p$. 故 $N(q) = 1$, 即 Sylow q- 子群 $\langle b \rangle$ 正规. 记 $\langle a \rangle$ 是 G 的 Sylow p- 子群, 于是

$$aba^{-1} = b^r, \quad r \in \{1, \cdots, q-1\}.$$

因为 $\langle a \rangle \langle b \rangle$ 的阶是 pq, 故 $G = \langle a \rangle \langle b \rangle$, 即 a, b 生成 G. 因此 $r \neq 1$ (否则, $ab = ba$, G 是 Abel 群). 又因

$$b = a^p ba^{-p} = b^{r^p},$$

故 $r^p \equiv 1 (\mathrm{mod}\ q)$. 注意到 $\langle a \rangle$ 不是正规子群 (否则 $G = \langle a \rangle \times \langle b \rangle$ 是 Abel 群), 因此 Sylow p- 子群的个数 $N(p) = kp + 1 = q$, 即 $p|q-1$.

于是 G 是由 a, b 生成, 满足

$$a^p = 1 = b^q,\ a^{-1}ba = b^r,\ r^p \equiv 1\ (\mathrm{mod}\ q),\ q \text{ 不整除 } r-1,\ p \text{ 整除 } q-1.$$

上面当然是定义关系, 这是标准的方法. 事实上, 令 $F = \langle x, y \rangle$ 是自由群, 并令 $\pi : F \longrightarrow G$ 是由 $\pi(x) = a, \pi(y) = b$ 给出的群同态. 则

$$\mathrm{Ker}\ \pi \supseteq \langle x^p, y^q, x^{-1}yxy^{-r} \rangle = K, \quad \text{且 } G \cong F/\mathrm{Ker}\ \pi.$$

因 $|F/K| = |F/\mathrm{Ker}\ \pi|\ |\mathrm{Ker}\ \pi/K| = pq|\mathrm{Ker}\ \pi/K|$, 又因 F/K 中的元形如

$$\overline{x}^i \overline{y}^j,\ 0 \leqslant i \leqslant p-1,\ 0 \leqslant j \leqslant q-1,$$

故 $|F/K| \leqslant pq$, 从而 $|\mathrm{Ker}\ \pi/K| = 1$, 即 $K = \mathrm{Ker}\ \pi$. 这表明上述关系是定义关系. ■

注 此题只是说若 G 是 pq 阶非 Abel 群, $p < q$, 则 G 的生成元和定义关系如上. 但上述证明并没有真正给出这样的群 G 的存在性, 这一点需要注意.

1.11.7*. 设 p 是奇素数, 试证 p^3 阶非 Abel 群 G 可以由下述生成元和定义关系给出:

(1) $G = \langle a, b \mid a^{p^2} = b^p = 1,\ b^{-1}ab = a^{1+p} \rangle$.

(2) $G = \langle a, b, c \mid a^p = b^p = c^p = 1,\ ac = ca,\ cb = bc,\ ab = bac \rangle$.

证 情形 I: 设 G 不含 p^2 阶元. 因 G 非 Abel 群, 故 $Z(G)$ 是 p 阶群. $G/Z(G)$ 是 p^2 阶群且非循环群. 设 $G/Z(G)\cong\langle\overline{a}\rangle\oplus\langle\overline{b}\rangle$, 其中 $\overline{a}$ 与 $\overline{b}$ 的阶均是 p. 因 G 不含 p^2 阶元, 故 a 与 b 的阶均是 p, 且

$$a^{-1}b^{-1}ab=c\in Z(G).$$

因为 $a,b,Z(G)$ 生成 G, 故 $c\neq 1$, 从而 $Z(G)=\langle c\rangle$. 于是 a,b,c 生成 G 且

$$a^p=b^p=c^p=1, ac=ca, bc=cb, ab=bac.$$

下证上述关系就是 G 的定义关系, 这是标准的方法.

设 $F=\langle x,y,z\rangle$ 是自由群. 令 $\pi:F\longrightarrow G$, $\pi(x)=a$, $\pi(y)=b$, $\pi(z)=c$ 为群同态. 则 $\mathrm{Ker}\ \pi\supseteq\langle x^p,y^p,z^p,xzx^{-1}z^{-1},yzy^{-1}z^{-1},x^{-1}y^{-1}xyz^{-1}\rangle=K$, 且 $G\cong F/\mathrm{Ker}\ \pi$.

因 $|F/K|=|F/\mathrm{Ker}\ \pi|\ |\mathrm{Ker}\ \pi/K|=p^3|\mathrm{Ker}\ \pi/K|$, 又因 F/K 中的元形如

$$\overline{x}^i\overline{y}^j\overline{z}^k, i,j,k\in\{0,1,\cdots,p-1\}.$$

故 $|F/K|\leqslant p^3$, 从而 $\mathrm{Ker}\ \pi=K$. 即上述关系是定义关系.

情形 II: 设 G 含有 p^2 阶元 a. 由题 1.11.3 知, $A=\langle a\rangle$ 是 G 的正规子群, 故 $G/\langle a\rangle=\langle\overline{b}\rangle$ 是 p 元群. 因此 b 不属于 A, $b^p\in A$. 设 $b^{-1}ab=a^r$, $r\in\{1,\cdots,p^2-1\}$. 因 a, b 生成 G, G 非 Abel 群, 故 $r\neq 1$. 易证

$$b^{-i}ab^i=a^{r^i}.$$

又 $a=b^{-p}ab^p=a^{r^p}$, 故 $r^p\equiv 1(\mathrm{mod}\ p^2)$. 因 $(r,p)=1$, 故 $r^{p-1}\equiv 1(\mathrm{mod}\ p)$, 从而 $r^p=r(\mathrm{mod}\ p)$.

因此 $r\equiv 1(\mathrm{mod}\ p)$. 记 $r=1+tp$, $t\in\{1,\cdots,p-1\}$.

因 $(t,p)=1$, 故存在 j 使得 $jt\equiv 1(\mathrm{mod}\ p)$. 从而

$$b^{-j}ab^j=a^{r^j}=a^{(1+tp)^j}=a^{1+jtp}=a^{1+p}.$$

因 $(j,p)=1$, 故 b^j 也不属于 A. 用 b^j 代替 b, 则有

$$a^{p^2}=1, b\ \text{不属于} A, b^p\in A, b^{-1}ab=a^{1+p}.$$

设 $b^p=a^s$. 因 b 的阶不能是 p^3, 即 b 的阶为 p 或 p^2, 故 $b^p=a^s$ 的阶是 p 或 1. 于是 s 是 p 的倍数. 令 $b^p=a^{up}$, 则由 $a^ib=ba^{(1+p)i}$ 知

$$(ba^{-u})^p=b^pa^{-u[1+(1+p)+(1+p)^2+\cdots+(1+p)^{p-1}]}.$$

因 $1+(1+p)+(1+p)^2+\cdots+(1+p)^{p-1}=\dfrac{(p+1)^p-1}{p}\equiv p\pmod{p^2}$, 故 $(ba^{-u})^p=b^pa^{-up}=1$. 令 $c=ba^{-u}$, 则 c 不属于 A.

于是 $c^p=1$, $c^{-1}ac=a^u(b^{-1}ab)a^{-u}=a^{1+p}$. 从而 G 由 p^2 阶元 a 与 p 阶元 c 生成, 满足 $ac=ca^{1+p}$.

令 $F=\langle x,y\rangle$ 是自由群, 并令 $\pi:F\longrightarrow G$ 是由 $\pi(x)=a$, $\pi(y)=c$ 给出的满同态. 则 $\mathrm{Ker}\ \pi\supseteq\langle x^{p^2},y^p,xyx^{-(1+p)}y^{-1}\rangle=K$ 且 $G\cong F/\mathrm{Ker}\ \pi$. 类似于情形 I 可知 $\mathrm{Ker}\ \pi=K$, 即上述关系是定义关系. ■

注　要说明上述关系真的定义了 p^3 阶非 Abel 群, 还要举出具体的例子.

§12　可解群和幂零群

知识要点:

换位子群; 商群可换的条件; 对称群 S_n 和交错群 A_n 的换位子群.

可解群的定义与性质; 可解群的等价定义; S_n 是可解群当且仅当 $n\leqslant 4$; A_n 是可解群当且仅当 $n\leqslant 4$.

幂零群的定义、例子、性质.

1.12.1. 设 $I^{(1)}(G)$ 是 G 的内自同构群, $I^{(n)}(G)$ 是 $I^{(n-1)}(G)$ 的内自同构群. 试证: G 是幂零群当且仅当存在 $n\geqslant 1$ 使得 $I^{(n)}(G)=\{1\}$.

证　$I^{(1)}(G)\cong G/Z(G)$.

$I^{(2)}(G)=I^{(1)}(I^{(1)}(G))\cong I^{(1)}(G)/Z(I^{(1)}(G))=(G/Z(G))/(Z(G/Z(G)))=G/Z_2(G)$.

归纳可证 $I^{(n)}(G)\cong G/Z_n(G)$. 因此, G 幂零 $\Longleftrightarrow$ 存在 $n\geqslant 1$ 使得 $Z_n(G)=G\Longleftrightarrow$ 存在 $n\geqslant 1$ 使得 $I^{(n)}(G)=\{1\}$. ■

1.12.2. 设 a 和 b 是有限幂零群 G 的两个元, $a^m=b^n=1$ 且 $(m,n)=1$. 试证 $ab=ba$.

证　有限幂零群是其 Sylow 子群的直积, 故 $G=G_1\times\cdots\times G_t$, 其中 G_i 是阶为 $p_i^{r_i}$ 的 Sylow 子群, $i=1,\cdots,t$. 设 $a\neq 1\neq b$, $o(a)$ 的素因子为 $\{p_1,\cdots,p_s\}$. 因 $a^m=1=b^n$, $(m,n)=1$, 故 $(o(a),o(b))=1$, 从而 $s<t$ 且 $o(b)$ 的素因子含于 $\{p_{s+1},\cdots,p_t\}$. 令 $H=G_1\times\cdots\times G_s$, $K=G_{s+1}\times\cdots\times G_t$, 则 $a\in H$, $b\in K$. 于是 $ab=ba$. ■

1.12.3. 设 G 是有限幂零群, 试证:

(1) 如果 $\{1\}\neq N\lhd G$, 则 $N\bigcap Z(G)\neq\{1\}$.

(2) 设 G 是非 Abel 群, A 是 G 的正规子群集合中的极大元, 且 A 是 Abel 群, 则 $C_G(A)=A$.

证 (1) 因 G 是有限幂零群, 故 $G = Z_n(G)$, 故 $N \bigcap Z_n(G) = N$. 下证 $N \bigcap Z_{n-1}(G) \neq \{1\}$.

$\forall n \in N, g \in G$, 因 $\overline{n} \in G/Z_{n-1}(G) = Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$, 故 $ngn^{-1}g^{-1} \in N \bigcap Z_{n-1}(G)$. 若 $N \bigcap Z_{n-1}(G) = \{1\}$, 则 $n \in Z(G)$, 即 $N \leqslant Z(G)$. 从而 $N \bigcap Z_{n-1}(G) = N \neq \{1\}$.

继续这个过程可得到 $N \bigcap Z(G) \neq \{1\}$.

(2) 因 A 是 Abel 群, 故 $A \leqslant C_G(A)$. 下证 $C_G(A)$ 是 G 的正规子群. $\forall g \in G,\ b \in C_G(A),\ \ x \in A$, 要证

$$gbg^{-1}x = xgbg^{-1}, \quad \text{即要证} \ \ gbg^{-1}xgb^{-1}g^{-1}x^{-1} = 1.$$

因 A 是 G 的正规子群, 故 $g^{-1}xg$ 与 b 可换. 从而有

$$gb(g^{-1}xg)b^{-1}g^{-1}x^{-1} = g(g^{-1}xg)bb^{-1}g^{-1}x^{-1} = xgg^{-1}x^{-1} = 1.$$

因 A 是 G 的正规子群集合中的极大元, 故 $C_G(A) = G$ 或 $C_G(A) = A$. 若 $C_G(A) = G$, 则 $A \leqslant Z(G)$. 从而 $Z(G) = A$ 或 $Z(G) = G$. 但 G 是非 Abel 群, 故 $Z(G) = A$. 因 G 是非可交换的幂零群, 故 $Z_2(G)$ 严格包含 $Z(G) = A$. 从而 $Z_2(G) = G$, 即 G/A 是 Abel 群. 但因 A 是 G 的正规子群集合中的极大元, 故 G/A 无非平凡的子群, 即 G/A 是素数阶循环群, 从而 G 是 Abel 群. 矛盾! 因此必有 $C_G(A) = A$. ■

注 由上述证明可知: 若 G 是非 Abel 群, A 是 G 的极大子群, 且 A 是 Abel 群, 则 $C_G(A) = A$.

1.12.4. 设 a, b 是群 G 的任意两个元. 如果 a, b 和它们的换位子 $[a, b]$ 可交换, 则对任意整数 m 和 n, $[a^m, b^n] = [a, b]^{mn}$.

证 首先, 对 n 用归纳法证明 $[a, b^n] = [a, b]^n$.

利用 $ab = [a, b]ba$ 可知

$$\begin{aligned}
[a, b^n] &= ab^na^{-1}b^{-n} = ab^{n-1}ba^{-1}b^{-n} \\
&= [a, b^{n-1}]b^{n-1}aba^{-1}b^{-n} = [a, b^{n-1}]b^{n-1}[a, b]b^{-n+1} \\
&= [a, b^{n-1}][a, b]b^{n-1}b^{-n+1} = [a, b^{n-1}][a, b] \\
&= [a, b]^{n-1}[a, b] = [a, b]^n.
\end{aligned}$$

再对 $m+n$ 用归纳法证 $[a^m, n^n] = [a,b]^{mn}$.

$$\begin{aligned}[a^m, b^n] &= a^m b^n a^{-m} b^{-n} = aa^{m-1} b^n a^{-m} b^{-n} \\ &= a[a^{m-1}, b^n] b^n a^{m-1} a^{-m} b^{-n} = [a^{m-1}, b^n] a b^n a^{-1} b^{-n} \\ &= [a^{m-1}, b^n][a, b^n] = [a,b]^{(m-1)n+n} \\ &= [a,b]^{mn}.\end{aligned}$$

■

1.12.5. 设 A, B 是群 G 的两个子群, $[A,B]$ 表示由 $\{[a,b] \mid a \in A, b \in B\}$ 生成的群, $\langle A,B\rangle$ 表示由 $A\bigcup B$ 生成的群. 试证:

(1) $[A,B] \lhd \langle A,B\rangle$.

(2) $A \lhd G$ 当且仅当 $[A,G] \leqslant A$.

(3) 如果 $B \lhd G$ 且 $B \leqslant A$, 则 $A/B \leqslant Z(G/B)$ 当且仅当 $[A,G] \leqslant B$.

证 (1) 只要证 $x[a,b]x^{-1} \in [A,B]$, $\forall a \in A$, $b \in B$, $x \in A\bigcup B$. 若 $x \in A$, 则

$$x[a,b]x^{-1} = [xa,b][x,b]^{-1} \in [A,B].$$

同理对 $x \in B$.

(2) 和 (3) 由定义可直接得到. ■

1.12.6. 对任意群 G, 定义 $r_1(G) = G$, $r_2(G) = [G,G]$, 一般地, $r_n(G) = [r_{n-1}(G), G]$. 试证: G 是幂零群当且仅当存在 $n \geqslant 1$ 使得 $r_n(G) = \{1\}$.

证 由定义知 $Z_1[G] = Z(G)$,

$$Z_{i+1}(G) = \{g \in G \mid [g,G] \leqslant Z_i(G)\}.$$

特别地 $[Z_{i+1}(G), G] \leqslant Z_i(G)$, $\forall i = 1,2,\cdots$.

若 G 幂零, 则 $Z_n(G) = G$. 于是 $r_1(G) \leqslant Z_n(G)$, 而 $r_2(G) = [r_1(G), G] \leqslant [Z_n(G), G] \leqslant Z_{n-1}(G)$. 一般地,

$$r_i(G) \leqslant Z_{n-i+1}(G).$$

于是 $r_n(G) \leqslant Z(G)$, 从而

$$r_{n+1}(G) = [r_n(G), G] \leqslant [Z(G), G] = \{1\}.$$

反之, 若 $r_n(G) = \{1\}$, 则 $r_{n-1}(G) \leqslant Z(G) = Z_1(G)$. 同样用归纳法可知 $r_{n-i}(G) \leqslant Z_i(G)$. 特别地 $G = r_1(G) \leqslant Z_{n-1}(G)$, 即 $Z_{n-1}(G) = G$, G 幂零. ■

1.12.7. 求二面体群 D_n 的换位子群, 这里 $D_n = \langle a, b \mid a^n = b^2 = 1, b^{-1}ab = a^{-1}\rangle$.

解

$$\begin{aligned}[a^ib^j, a^sb^t] &= a^ib^ja^sb^tb^{-j}a^{-i}b^{-t}a^{-s} \\ &= a^i(b^ja^sb^{-j})(b^ta^{-i}b^{-t})a^{-s} \\ &= a^i(b^jab^{-j})^s(b^tab^{-t})^{-i}a^{-s} \\ &= a^ia^{(-1)^js}a^{(-1)^t(-i)}a^{-s} \\ &= a^{i\pm s\pm i-s} \in \langle a^2\rangle,\end{aligned}$$

因此 $D_n' = \langle a^2\rangle$. ■

1.12.8. 试证: 对称群 S_3 和 S_4 是可解群, 但不是幂零群.

证　$S_3' = A_3$,　$A_3' = (1)$.　$S_4' = A_4$,　$A_4' = K_4$,　$K_4' = (1)$. 故 S_3, S_4 是可解群.

$Z(S_3) = 1 = Z(S_4)$, 故 S_3, S_4 非幂零. ■

1.12.9. 设 $N \lhd G$. 如果 N 和 G/N 均为幂零群, G 是否为幂零群?

解　否. 例如, S_3 的正规子群 A_3 幂零, S_3/A_3 幂零, 但 S_3 非幂零. ■

1.12.10. 设 $N \leqslant Z(G)$, 试证: 如果 G/N 为幂零群, 则 G 为幂零群.

证　注意到 $Z_n(G/N) = Z_n(G)/N$, 这里 $N \leqslant Z(G)$. 因此, 若 $Z_n(G/N) = G/N$, 则 $Z_n(G) = G$. ■

1.12.11. 设 $G = S_4$, 试证 $G/G^{(2)} \cong S_3$.

证　$S_4' = A_4$,　$S_4^{(2)} = K_4$.　S_4/K_4 是非可交换的 6 阶群, 因此 $S_4/K_4 \cong S_3$. ■

1.12.12. 设 A 是群 G 的循环的正规子群. 试证 A 和 G' 按元可交换, 即对任意 $a \in A$, $x \in G'$, $ax = xa$.

证　设 $A = \langle a\rangle$. $\forall g \in G$, 设 $g^{-1}ag = a^{n(g)}$. 要证 $aghg^{-1}h^{-1} = ghg^{-1}h^{-1}a$, $\forall g, h \in G$. 即要证 $h^{-1}g^{-1}agh = g^{-1}h^{-1}ahg$. 即 $h^{-1}a^{n(g)}h = g^{-1}a^{n(h)}g$, 即 $a^{n(g)n(h)} = a^{n(h)n(g)}$, 这当然是正确的. ■

1.12.13. 设 α 是群 G 的一个自同构. 如果对任意 $g \in G$, $g^{-1}\alpha(g) \in Z(G)$, 则对导群 G' 的任意元 a, $\alpha(a) = a$.

证　因 $g^{-1}\alpha(g) \in Z(G)$, 故 $\alpha(g) = gc$, $c \in Z(G)$. 因此对 $\forall g, h \in G$, 存在

$c_1, c_2 \in Z(G)$, 使得

$$\begin{aligned}\alpha(ghg^{-1}h^{-1}) &= \alpha(g)\alpha(h)\alpha(g)^{-1}\alpha(h)^{-1}\\ &= gc_1hc_2c_1^{-1}g^{-1}c_2^{-1}h^{-1}\\ &= ghg^{-1}h^{-1},\end{aligned}$$

即 α 在 G' 上为恒等映射. ■

1.12.14. 设 p, q, r 是三个素数, 不一定不相同, 试证: pqr 阶群是可解群.

证 首先, p^3 阶群可解. 其次, pq 阶群可解 $(p \neq q)$. 接下来, p^2q 阶群可解.

现在设 $|G| = p\cdot q\cdot r$, $p > q > r$. 只要证 G 非单 (设 $N \lhd G$, $N \neq (1)$, $N \neq G$, 则由归纳假设 N 可解, G/N 可解, 故 G 可解).

否则, 设 G 单. 则 Sylow p- 子群的个数为 qr, Sylow q- 子群的个数为 pr 或 p, Sylow r- 子群的个数为 pq, p 或 q. 无论哪种情形, 均有矛盾:

$$\begin{aligned}|G| &\geqslant qr(p-1) + p(q-1) + q(r-1) + 1\\ &= pqr + pq - p - q + 1 = pqr + (p-1)(q-1)\\ &> pqr.\end{aligned}$$ ■

注 事实上, 由本题的证明知, 若 p, q, r 是三个素数 (不一定不相同), 则 pqr 阶群非单.

1.12.15. 有限群 G 是可解群当且仅当 G 的合成因子均是素数阶循环群.

证 若 G 的合成因子均是素数阶循环群, 则易知 G 可解.

反之, 设 G 可解. 考虑 G 的合成列, 则每个合成因子 G_i/G_{i+1} 均是单群. 因 G 可解, 故作为 G 的子群的商群 G_i/G_{i+1} 也可解, 从而 G_i/G_{i+1} 的导群应严格小于 G_i/G_{i+1}, 故它只能是 $\{1\}$. 从而 G_i/G_{i+1} 是 Abel 群. 又 G_i/G_{i+1} 单, 故 G_i/G_{i+1} 只能是素数阶的循环群. ■

1.12.16. (1) 求 S_4 的导出列、合成列和合成因子.

(2) 求四元数群 Q_8 的所有合成列.

解 (1) 导出列: $S_4 \rhd A_4 \rhd K_4 \rhd \{1\}$.

合成列: $S_4 \rhd A_4 \rhd K_4 \rhd \mathbb{Z}_2 \rhd \{1\}$.

合成因子: $\mathbb{Z}_2, \mathbb{Z}_3$, $\mathbb{Z}_2, \mathbb{Z}_2$.

(2) $Q_8 \rhd \langle a\rangle \rhd \langle a^2\rangle \rhd \{1\}$,

$Q_8 \rhd \langle b\rangle \rhd \langle a^2\rangle \rhd \{1\}$,

$Q_8 \rhd \langle ab\rangle \rhd \langle a^2\rangle \rhd \{1\}$. ■

1.12.17. 设 G 是 p^3 阶非交换群, p 为素数. 则 $Z(G)=G^{(1)}$.

证 因 G 有非平凡的中心且非可换, 故 $1<|Z(G)|<p^3$. 又 $|Z(G)|\neq p^2$ (否则 $G/Z(G)$ 是循环群, 从而 G 可换), 故 $|Z(G)|=p$. 于是 $G/Z(G)$ 是 p^2 阶群, 从而可换. 于是 $G^{(1)}\subseteq Z(G)$. 但 $G^{(1)}\neq\{1\}$ (否则 G 可换), 因此 $Z(G)=G^{(1)}$. ■

1.12.18. 求对称群 S_n 和交错群 A_n 的导出列.

解 设 $n\geqslant 5$. 因 $S_n/A_n\cong\mathbb{Z}_2$, 故 $A_n\supseteq S_n^{(1)}$. 但 A_n $(n\geqslant 5)$ 是单群, 故 $S_n^{(1)}=A_n$ 或 $S_n^{(1)}=\{1\}$. 又 S_n 不是可换群, 故 $S_n^{(1)}=A_n$. 同理 $A_n^{(1)}=A_n$.

因此, 当 $n\geqslant 5$ 时, S_n 的导出列为 $S_n\rhd A_n\rhd A_n\rhd\cdots$.

A_n 的导出列为 $A_n\rhd A_n\rhd\cdots$.

S_4 的导出列为 $S_4\rhd A_4\rhd K_4\rhd\{1\}$.

A_4 的导出列为 $A_4\rhd K_4\rhd\{1\}$.

S_3 的导出列为 $S_3\rhd A_3\rhd\{1\}$.

A_3 的导出列为 $A_3\rhd\{1\}$. ■

1.12.19. 阶为素数幂的群 G 是可解群.

证 设 $|G|=p^n$, $n\geqslant 1$. 对 n 用数学归纳法. 若 $n=1$, 则 G 是素数阶循环群, 从而是可解群. 设 $n>1$. 因 G 的中心 $C(G)\neq\{1\}$, 故 $G/C(G)$ 的阶为 p^m, $m<n$. 由归纳假设 $G/C(G)$ 是可解群. 又 $C(G)$ 是 Abel 群, 从而是 $C(G)$ 可解群. 于是 $G/C(G)$ 与 $C(G)$ 均是可解群, 从而 G 是可解群. ■

1.12.20. 对于有限群 G 来说, 下述命题等价:

(1) G 是可解群, 即有正整数 n 使得 $G^{(n)}=\{1\}$, 其中 $G^{(n)}$ 是 G 的第 n 次导群.

(2) G 有终止于 $\{1\}$ 的正规群列, 即存在 $G=G_0\rhd G_1\rhd\cdots\rhd G_m=\{1\}$, 且 $G_i\lhd G$, $1\leqslant i\leqslant m$, 使得每个因子群 G_{i-1}/G_i 均为 Abel 群, $1\leqslant i\leqslant m$.

(3) G 有终止于 $\{1\}$ 的次正规群列, 即存在 $G=G_0\rhd G_1\rhd\cdots\rhd G_m=\{1\}$, 使得每个因子群 G_{i-1}/G_i 均为 Abel 群, $1\leqslant i\leqslant m$.

(4) G 有终止于 $\{1\}$ 的次正规群列, 使得每个因子群均为素数阶循环群.

(5) G 有终止于 $\{1\}$ 的次正规群列, 使得每个因子群的阶均为素数幂.

证 (1) $\Longrightarrow$ (2): 取导出列.

(2) $\Longrightarrow$ (3): 显然.

(3) $\Longrightarrow$ (4): 由有限 Abel 群的结构定理可推知.

(4) $\Longrightarrow$ (5): 显然.

(5) $\Longrightarrow$ (1): 阶为素数幂的群是可解群. 由题设, G 是可解群借助可解群的反复扩张, 故 G 是可解群. ■

注　(1) 上述 (4) 中的次正规群列不可以改为正规群列.

例如 S_4 有次正规群列

$$S_4 \rhd A_4 \rhd K_4 \rhd \mathbb{Z}_2 \rhd \{1\}$$

使得每个因子群均为素数阶循环群, 但却没有终止于 $\{1\}$ 的正规群列使得每个因子群均为素数阶循环群.

(2) 上述 (5) 中的次正规群列可以改为正规群列. 不过, 证明要长得多, 需要用到特征单群的概念与方法. 此处从略.

第 2 章　环　论

§1　基 本 概 念

知识要点:

环、交换环、环中 (左、右) 零因子、整环、除环 (或称为体)、域的定义; 环的简单性质; 环的基本例子: 数环、剩余类环、矩阵环、多项式环、加法群的自同态环、群环、四元数体; 环同态与环同构; 环的自同构群.

注　本书中环未必有单位元 (或称为幺元). 有单位元的环以下称为含幺环.

2.1.1.　设 A 是 Abel 群, $\mathrm{End}(A)$ 是群 A 的全部自同态作成的集合. 对 f, $g \in \mathrm{End}(A)$ 定义

$$(f+g)(a) = f(a)+g(a), \quad (f\cdot g)(a) = f(g(a)), \quad \forall\, a \in A.$$

则 $\mathrm{End}(A)$ 对于上述运算是含幺环.

证　由定义直接验证, 其中 $\mathrm{End}(A)$ 的零元是零映射, 单位元是恒等映射. ■

2.1.2.　(1)* 举例表明含幺环中, 一个左可逆元可以具有多于一个左逆.

(2)　如果 a 是含幺环中左可逆元, 并且 a 不是右零因子, 则 a 只有唯一的左逆.

证　(1) 令 A 是无穷实数列 $\{a_0, a_1, a_2, \cdots\}$ 的集合, 则 A 对于分量加法作成 Abel 群. 考虑 A 的自同态环 $\mathrm{End}(A)$, 记为 R, 则 R 有单位元 id. 令 $r \in R$ 为右平移变换, 即

$$r(\{a_0, a_1, a_2, \cdots\}) = \{0, a_0, a_1, \cdots\}.$$

令 $l \in R$ 为左平移变换, 即

$$l(\{a_0, a_1, a_2, \cdots\}) = \{a_1, a_2, a_3, \cdots\}.$$

令 $l_0 : A \longrightarrow A$ 是由

$$l_0(\{a_0, a_1, a_2, \cdots\}) = \{a_0 + a_1, a_2, a_3, \cdots\}$$

给出的变换, 则 $l_0 \in R$. 显然有 $lr = \mathrm{id} = l_0 r$, 即 l 和 l_0 均为左可逆元 r 的左逆, 且 $l \neq l_0$.

(2) 由定义直接反证. ■

2.1.3.　设 a 是环 R 中非零元, 求证:

(1)　a 不是 R 中左零因子当且仅当由等式 $ab = ac$, 其中 $b, c \in R$ 可推出

$b = c$.

(2) a 不是 R 中右零因子当且仅当由等式 $ba = ca$, 其中 $b, c \in R$ 可推出 $b = c$.

证 由定义直接推证. ■

2.1.4. 设 $n \geqslant 2$ 为正整数, 求证:

(1) 环 $\mathbb{Z}_n$ 中元 $\bar{a}$ 可逆当且仅当 $(a, n) = 1$.

(2) 若 p 为素数, 则 $\mathbb{Z}_p$ 是域; 若 n 不是素数, 则 $\mathbb{Z}_n$ 不是整环.

证 (1) $(a, n) = 1$ 当且仅当存在整数 l 和 m, 使得 $la + mn = 1$; 当且仅当存在整数 l 使得在 $\mathbb{Z}_n$ 中, $\bar{l}\,\bar{a} = \bar{1}$; 当且仅当 $\bar{a}$ 在 $\mathbb{Z}_n$ 中可逆.

(2) 第一个结论由 (1) 即知.

设 n 不是素数, 则存在大于 1 的整数 s, t, 使得 $st = n$. 于是 $\bar{s} \neq \bar{0} \neq \bar{t}$, 而 $\bar{s}\bar{t} = \bar{0}$. 从而 $\mathbb{Z}_n$ 不是整环. ■

2.1.5. (1) 决定环 $\mathbb{Z}[\sqrt{-1}\,]$ 的单位群, 证明此环为整环但不是域.

(2) 对于环 $\mathbb{Z}[\sqrt{-3}\,] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ 做同样事情.

证 (1) 若 $(a+b\mathrm{i})(c+d\mathrm{i}) = 1$, 则 $(a^2+b^2)(c^2+d^2) = 1$, $a, b, c, d \in \mathbb{Z}$. 从而 $a = \pm 1$, $b = 0$; 或者 $a = 0$, $b = \pm 1$. 因此 $\mathbb{Z}[\sqrt{-1}]$ 的单位群为 $\{1, -1, \mathrm{i}, -\mathrm{i}\} = \langle \mathrm{i} \rangle$.

(2) 同理可知 $\mathbb{Z}[\sqrt{-3}\,]$ 的单位群为 $\{1, -1\}$. ■

2.1.6. 设 R 和 S 均为含幺环, $f: R \longrightarrow S$ 为环的满同态. 则

(1) $f(1_R) = 1_S$.

(2) 设 $0_S \neq 1_S$, 如果 $a \in U(R)$, 则 $f(a) \in U(S)$, 并且 $f(a^{-1}) = f(a)^{-1}$.

证 由定义直接推证. 注意 (1) 中要用到 f 是满射的条件. ■

2.1.7. 设 G 是乘法群, R 为环. 定义集合 $R[G] = \left\{ \sum\limits_{g \in G} r_g g \mid r_g \in R, \text{并且只有有限多个 } r_g \neq 0 \right\}$. 规定 $R[G]$ 中两个元 $\sum\limits_{g \in G} r_g g$ 和 $\sum\limits_{g \in G} t_g g$ 相等当且仅当 $r_g = t_g$, $\forall\, g \in G$. 在集合 $R[G]$ 上定义

$$\sum_{g \in G} r_g g + \sum_{g \in G} t_g g = \sum_{g \in G} (r_g + t_g) g,$$

$$\left(\sum_{g \in G} r_g g \right) \left(\sum_{g \in G} t_g g \right) = \sum_{g \in G} \left(\sum_{g'g''=g} r_{g'} t_{g''} \right) g.$$

(1) $R[G]$ 对于上述加法和乘法作成环 (叫做群 G 在环 R 上的群环).

(2) $R[G]$ 是交换环当且仅当 R 是交换环且 G 是 Abel 群.

(3) 若环 R 有单位元 1_R, 而群 G 的单位元为 e, 则 $1_R e$ 是群环 $R[G]$ 的幺元.

(4) R 可以自然地看成是 $R[G]$ 的子环.

(5) 设 G 是有限群, R 是交换环. 求群环 $R[G]$ 的中心 $Z(R[G])$.

(6) $R[G]$ 是否为无零因子环?

证 (1)—(4) 由定义直接推证.

(5) 令 $S_g = \sum_{x\in G} xgx^{-1}$, $\widetilde{S_g} = \sum_{h\in[g]} h$, 其中 $[g]$ 表示 g 所在的共轭类. 注意到 $S_g = [G : C_G(g)]\widetilde{S_g}$.

由定义易证: $Z(R[G]) = R\widetilde{S_{g_1}} + R\widetilde{S_{g_2}} + \cdots + R\widetilde{S_{g_t}}$, 其中 $\{g_1, \cdots, g_t\}$ 是 G 的共轭类的一个代表元系.

(6) 因为

$$\sum_{g\in G} g(1-h) = (1-h)\sum_{g\in G} g = 0,\ \forall\, h \in G,$$

故当 $G \neq \{1\}$ 时, $1-h$ 与 $\sum_{g\in G} g$ 均为 G 的零因子; 而当 $G = \{1\}$ 时, $R[G]$ 是无零因子环当且仅当 R 是无零因子环. ■

2.1.8. (1) 整数环 $\mathbb{Z}$ 的加法群自同构是否一定为环的自同构?

(2) 求 $\mathbb{Z}_m$ 的全部子环和 $\mathrm{Aut}(\mathbb{Z}_m)$, 其中 m 为正整数.

证 (1) 否. 加法群 $\mathbb{Z}$ 的自同构群为 $\mathbb{Z}_2$, 而环 $\mathbb{Z}$ 的自同构只能是恒等.

(2) $\mathbb{Z}_m$ 的子环必为循环群 $\mathbb{Z}_m$ 的子群, 从而形如 $\mathbb{Z}_r$, 其中 r 为 m 的正因子. 注意 $\mathbb{Z}_1 = 0$. 因此 $\mathbb{Z}_m$ 的全部子环为 $\mathbb{Z}_r \cong \frac{m}{r}\mathbb{Z}_m$, 其中 r 取遍 m 的正因子.

设 $\pi \in \mathrm{Aut}(\mathbb{Z}_m)$, 则 $\pi(\overline{1}) = \overline{1}$. 因此 $\pi(x) = x$, $\forall\, x \in \mathbb{Z}_m$. 故 $\mathrm{Aut}(\mathbb{Z}_m) = \{1\}$. ■

2.1.9. (1) 求 $\mathbb{Q}$ 的全部子域.

(2) 求证 $\mathbb{Q}[\sqrt{2}\,] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 是实数域 $\mathbb{R}$ 的子域; 并求 $\mathbb{Q}[\sqrt{2}\,]$ 的全部子域.

(3) 求 $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}\,])$.

证 (1) $\mathbb{Q}$ 的子域只有 $\mathbb{Q}$ 本身.

(2) 由定义直接验证 $\mathbb{Q}[\sqrt{2}\,]$ 是 $\mathbb{R}$ 的子域. 注意 $\mathbb{Z}[\sqrt{2}\,]$ 不是域.

$\mathbb{Q}[\sqrt{2}\,]$ 的任意子域 T 必然包含 $\mathbb{Q}$, 若 T 还含有 $a + b\sqrt{2}$, $b \neq 0$, 则 $\sqrt{2} \in T$. 从而 $T = \mathbb{Q}[\sqrt{2}\,]$. 即 $\mathbb{Q}[\sqrt{2}\,]$ 的子域为 $\mathbb{Q}$ 和 $\mathbb{Q}[\sqrt{2}\,]$.

(3) 设 $\pi \in \mathrm{Aut}(\mathbb{Q}[\sqrt{2}\,])$, 则 $\pi(1) = 1$. 因此 π 在 $\mathbb{Q}$ 上的限制是恒等. 设 $\pi(\sqrt{2}) = a$, 则 $a^2 = 2$, 即 $\pi(\sqrt{2}) = \pm\sqrt{2}$. 由此可知, $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}]) = \{\mathrm{id}, \alpha\} \cong \mathbb{Z}_2$, 其中 $\alpha(a + b\sqrt{2}) = a - b\sqrt{2}$, $\forall\, a, b \in \mathbb{Q}$. ■

2.1.10*. (1) 设 $f \in \mathrm{Aut}(\mathbb{R})$, $\alpha, \beta \in \mathbb{R}$. 若 $\alpha > 0$, 则 $f(\alpha) > 0$. 从而, 若 $\alpha > \beta$, 则 $f(\alpha) > f(\beta)$.

(2) 求 $\mathrm{Aut}(\mathbb{R})$.

证 (1) 设 $\alpha > 0$, 则存在 $\beta \in \mathbb{R}$, 使得 $\alpha = \beta^2$. 于是 $f(\alpha) = (f(\beta))^2 > 0$.

(2) 设 $f \in \mathrm{Aut}(\mathbb{R})$. 因 $f(1) = 1$, 容易推知 f 在 $\mathbb{Q}$ 上的限制为恒等. 设 $r \in \mathbb{R}$, r 是无理数且 $r > 0$. 取有理单调递增数列 $\{r_n\}$ 使得 $\lim\limits_{n\to\infty} r_n = r$. 因此对任意大的正整数 N, 存在 N' 使得当 $n > N'$ 时, 有 $0 < r - r_n < \dfrac{1}{N}$. 从而

$$0 < f(r) - f(r_n) = f(r - r_n) < f\left(\frac{1}{N}\right) = \frac{1}{N}.$$

这表明 $f(r) = \lim\limits_{n\to\infty} r_n = r$. 从而 $\mathrm{Aut}(\mathbb{R}) = \{1\}$. ■

2.1.11. (1) 可将复数域 $\mathbb{C}$ 嵌到环 $M_2(\mathbb{R})$ 中吗?

(2) 令 $L = \left\{\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \middle| z, w \in \mathbb{C}\right\}$, 其中 $\overline{w}$ 为 w 的共轭复数, 求证 L 是体, 并且同构于实四元数体 $\mathbb{H}$.

证 (1) 令 $\sigma: \mathbb{C} \longrightarrow M_2(\mathbb{R})$, 其中 $\sigma(a+b\mathrm{i}) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. 则 σ 是环的嵌入.

(2) 令 $\pi: \mathbb{H} \longrightarrow L$, $\pi(a_0e + a_1i + a_2j + a_3k) = \begin{pmatrix} a_0 + a_1\mathrm{i} & a_2 + a_3\mathrm{i} \\ -a_2 + a_3\mathrm{i} & a_0 - a_1\mathrm{i} \end{pmatrix}$. 则可直接验证 π 是环同构. ■

2.1.12. 设 R 为环, 如果每个元 $a \in R$ 均满足 $a^2 = a$, 则称 R 为布尔 (Boole) 环. 求证:

(1) 布尔环 R 必为交换环, 并且 $a + a = 0_R$, $\forall\, a \in R$.

(2) 设 U 是一个集合, S 是 U 的全部子集构成的集族, 即 $S = \{V \mid V \subseteq U\}$. 对于 $A, B \in S$, 定义

$$A - B = \{c \in U \mid c \in A,\ c \notin B\},$$
$$A + B = (A - B)\bigcup(B - A),$$
$$A \cdot B = A\bigcap B.$$

求证 $(S, +, \cdot)$ 是布尔环. 环 S 是否有幺元?

证 (1) 因 $a + a = (a+a)^2 = a^2 + a + a + a^2 = a + a + a + a$, 故 $a + a = 0_R$, $\forall a \in R$.

因 $a+b=(a+b)^2=a^2+ab+ba+b^2=a+b+ab+ba$, 故 $ab=-ba=ba$, $\forall a,b\in R$, 即 R 为交换环.

(2) 直接验证. 环 S 有幺元 U. ■

2.1.13*. 试证:

(1) 有限整环必为域.

(2) 只有有限个理想的整环 R 是域.

证 (1) 有限整环 R 中非零元的集合对于乘法作成一个满足消去律的有限含幺半群, 从而是群. 因此 R 是域.

(2) 只要证 $R^*=R-0$ 是群; 进而只要证 $ax=b$ 在 R^* 中有解, $\forall\, a,b\in R^*$. 考虑 R 的理想 Ra, $Ra^2,\cdots$. 因 R 只有有限个理想, 故存在 $m<n$ 使得 $Ra^m=Ra^n$. 从而存在 $c\in R$ 使得 $ba^m=ca^n$. 故 $b=ca^{n-m}$. ■

2.1.14. 以 $C(\mathbb{R})$ 表示全部连续实函数 $f:\mathbb{R}\longrightarrow\mathbb{R}$ 组成的集合. 定义 $(f+g)(a)=f(a)+g(a)$, $(f\cdot g)(a)=f(a)\cdot g(a)$, 对于 $f,g\in C(\mathbb{R})$, $a\in\mathbb{R}$. 求证 $C(\mathbb{R})$ 由此成为含幺交换环. 试问 $C(\mathbb{R})$ 是否为整环? 是否有幂零元? 决定环 $C(\mathbb{R})$ 的单位群.

证 直接验证 $C(\mathbb{R})$ 是有单位元的交换环, 但非整环. 注意 $C(\mathbb{R})$ 与 $\mathrm{End}(\mathbb{R})$ 的区别.

$C(\mathbb{R})$ 无非零的幂零元. $C(\mathbb{R})$ 的单位群为 $\{f\in C(\mathbb{R})\mid f(a)\neq 0,\forall\, a\in\mathbb{R}\}$. ■

2.1.15. 设 D 为有限体, 求证 $a^{|D|}=a$, $\forall\, a\in D$.

证 设 D^* 是 D 的非零元作成的 $|D|-1$ 阶乘法群, 则 $a^{|D|-1}=1$, $\forall\, a\in D^*$. 由此即得. ■

2.1.16. 设 G 为二元群, 试决定群环 $\mathbb{Z}[G]$ 的单位群.

证 设 $G=\{1,g\}$, 则 $n+mg\in\mathbb{Z}[G]$ 可逆当且仅当存在 $x+yg\in\mathbb{Z}[G]$ 使得 $(n+mg)(x+yg)=1$. 这当且仅当齐次线性方程组

$$\begin{cases} nx+my=1,\\ mx+ny=0\end{cases}$$

有整数解, 当且仅当 $n^2-m^2=\pm1$. 由此可知 $\mathbb{Z}[G]$ 的单位群为 $\{1,-1,g,-g\}=K_4$. ■

2.1.17*. 设 a,b 是含幺环 R 中的元, 则 $1-ab$ 可逆 $\Longleftrightarrow$ $1-ba$ 可逆.

证 设 $1-ab$ 的逆元为 c, 则可验证 $1+bca$ 是 $1-ba$ 的逆元. ■

注 若 $x^n = 0$, 则 $1-x$ 的逆元为 $1+x+x^2+\cdots+x^{n-1}$. 因此形式上, 可将 $1-ab$ 的逆元想象为 $c = 1+ab+(ab)^2+\cdots$, 而将 $1-ba$ 的逆元想象为 $1+ba+(ba)^2+\cdots = 1+bca$, 然后再加以验证. ■

2.1.18*. (华罗庚) 设含幺环 R 中元 a, b, $1-ab$ 均为单位, 则 $a-b^{-1}$ 和 $(a-b^{-1})^{-1}-a^{-1}$ 也是单位, 且

$$((a-b^{-1})^{-1}-a^{-1})^{-1} = aba-a.$$

证 因 $a-b^{-1} = -(1-ab)b^{-1}$, 故 $a-b^{-1}$ 是单位.

用 $(a-b^{-1})^{-1}$ 和 a 分别代替 $a-b^{-1}$ 中的 a 和 b, 即得 $(a-b^{-1})^{-1}-a^{-1}$ 也是单位.

注意到 $(ab)^{-1}-1$ 也是单位, 且

$$(b^{-1}a^{-1}-1)^{-1} = (1-ab)^{-1}-1. \qquad (*)$$

事实上,

$$\begin{aligned}&(b^{-1}a^{-1}-1)((1-ab)^{-1}-1)(1-ab) = (b^{-1}a^{-1}-1)(1-(1-ab))\\&= (b^{-1}a^{-1}-1)(ab) = 1-ab,\end{aligned}$$

两边约去单位 $1-ab$ 得到 $(b^{-1}a^{-1}-1)((1-ab)^{-1}-1) = 1$. 同理有 $((1-ab)^{-1}-1)(b^{-1}a^{-1}-1) = 1$, 从而 $(*)$ 式成立.

将 $(*)$ 式两边左乘 a^{-1}, 得到 $(b^{-1}-a)^{-1} = (a-aba)^{-1}-a^{-1}$. 从而

$$((a-b^{-1})^{-1}-a^{-1})^{-1} = (a^{-1}-(a-aba)^{-1}-a^{-1})^{-1} = (-(a-aba)^{-1})^{-1} = aba-a. \ ■$$

注 事实上, 上述 $(*)$ 式说明了: 如果 x, $1-x$ 均是 R 中单位, 则 $x^{-1}-1$ 也是 R 中单位, 且有

$$(x^{-1}-1)^{-1} = (1-x)^{-1}-1.$$

2.1.19*. (Kaplansky) 含幺环中某元若有多于一个右逆, 则它必然有无限多个右逆.

证 设 $a \in R$ 有多于一个右逆, 则 a 是左零因子, 从而右理想 $I = \{x \in R \mid ax = 0\}$ 非零. 欲证 a 有无限多个右逆, 只要证 I 是无限集即可: 这是因为若 b 是 a 的一个右逆, 则 $b+x, \forall\, x \in I$ 均为 a 的右逆.

否则, 设 $I = \{x_0, x_1, x_2, \cdots, x_n\}$, 其中 $x_0 = 0$. 则 $x_ia \in I, i = 1, 2, \cdots, n$. 因 a 有右逆, 故 $x_ia \neq x_ja \neq 0, \forall\, i \neq j$. 因此 $\{x_1a, x_2a, \cdots, x_na\}$ 是 $\{x_1, x_2, \cdots, x_n\}$ 的一个置换. 设 b 是 a 的一个右逆, 则 $ba \neq 1$ (因 a 是左零因子). 于是 $ba-1 \in I$.

从而 $ba-1=x_i$, 且 $x_ib=(ba-1)b=0$. 但另一方面 $x_i=x_ja$, 从而 $x_ib=x_jab=x_j\neq 0$. 矛盾! ■

2.1.20*. (1) (华罗庚, 1949) 设 L 是非可换体, a 是 L 中非中心的元, 则 L 由 a 的所有共轭元生成.

(2) (H.Cartan-R.Brauer- 华罗庚) 设 L 是体, K 是其真子体, 且 $K^*=K-\{0\}$ 是 L^* 的正规子群, 则 K 含于 L 的中心.

证 (1) 设 x,y 是 L 中两个不可换的元, 则 $y(x-1)\neq(x-1)y$, 故 $y^{-1}\neq(x-1)^{-1}y^{-1}(x-1)$. 因此

$$
\begin{aligned}
&x(x^{-1}y^{-1}x-(x-1)^{-1}y^{-1}(x-1))\\
&=y^{-1}x-x(x-1)^{-1}y^{-1}(x-1)\\
&=y^{-1}x-(x-1+1)(x-1)^{-1}y^{-1}(x-1)\\
&=y^{-1}x-y^{-1}(x-1)-(x-1)^{-1}y^{-1}(x-1)\\
&=y^{-1}-(x-1)^{-1}y^{-1}(x-1)\\
&\neq 0.
\end{aligned}
$$

所以

$$x=(y^{-1}-(x-1)^{-1}y^{-1}(x-1))(x^{-1}y^{-1}x-(x-1)^{-1}y^{-1}(x-1))^{-1}. \qquad (*)$$

现在设 L_1 是 L 的由 a 的所有共轭元生成的子域. (反证) 假设 $L_1\neq L$, 则 $L-L_1$ 中任一元 x 与 a 的任一共轭元 y 均可换 (否则, 由 $(*)$ 式知 $x\in L_1$. 矛盾!), 于是 $L-L_1$ 中任一元与 L_1 中任一元均可换.

因 a 是非中心元, 故存在 $z\in L$ 与 a 不可换, 则由 $(*)$ 式知 $z\in L_1$, 取 $x\in L-L_1$, 则 $xz\notin L_1$. 于是 xz 与 a 可换, 从而

$$(xz)a=a(xz)=(ax)z=(xa)z.$$

约去 x, 得到矛盾 $za=az$!

(2) 若 K 不含于 L 的中心, 即 K 含有 L 的某个非中心元 a, 则由 (1) 知 L 由 a 的所有共轭元生成, 从而由题设知 $L=K$. ■

§2 环的同构定理

知识要点:

环的理想及其构造; 主理想整环; 除环上的全矩阵环是单环; 商环的构造; 环同态基本定理及其应用 (与群论的平行和区别).

2.2.1. 环 R 中的元 a 叫做幂零的, 是指存在正整数 m 使得 $a^m = 0$.

(1) 若 R 为交换环, a 和 b 均为幂零元, 则 $a+b$ 也是幂零元.

(2) 若 R 不为交换环,(1) 中结论是否仍成立?

(3) 交换环 R 中幂零元的集合 N 是 R 的理想, 且商环 R/N 中只有 0 是幂零元.

证 (1) 设 $a^m = 0$, $b^n = 0$. 因 $ab = ba$, 故 $(a+b)^{m+n} = \sum\limits_{i=0}^{m+n} \mathrm{C}_{m+n}^{i} a^i b^{m+n-i}$. 因为或者 $i \geqslant m$, 或者 $m+n-i \geqslant n$, 故 $a^i b^{m+n-i} = 0$, $0 \leqslant i \leqslant m+n$. 即 $(a+b)^{m+n} = 0$.

(2) 否. 例如, $M_2(\mathbb{R})$ 中 $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ 均为幂零元, 但 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 可逆.

(3) 由 (1) 可直接推出. ■

2.2.2. 设 I 是交换环 R 中的理想, 求证集合 $\sqrt{I} = \{r \in R \mid 存在\ n \geqslant 1使得\ r^n \in I\}$ 也是环 R 的理想.

证 类似于题 2.2.1(1) 的证明. ■

2.2.3. 设 R 为环, 集合 $Z(R) = \{c \in R \mid 对于每个\ r \in R,\ rc = cr\}$ 叫做环 R 的中心.

(1) 求证 $Z(R)$ 是 R 的子环, 但不一定是 R 的理想.

(2) 如果 F 为域, 求证全矩阵环 $M_n(F)$ 的中心为 $\{aI_n \mid a \in F\}$, 其中 I_n 表示 n 阶单位方阵.

证 (1) 直接验证 $Z(R)$ 是 R 的子环.

(2) 由线性代数知, 与域 F 上任一 n 阶矩阵都交换的 n 阶矩阵只能为 aI_n, $a \in F$. 因此 $Z(M_n(F)) = \{aI_n \mid a \in F\}$.

由此也可见: 环 R 的中心不一定是环 R 的理想. ■

2.2.4. (1)* 设 R 为含幺交换环, 求证环 $M_n(R)$ 中每个理想均为形式 $M_n(I)$, 其中 I 是 R 的某个理想.

(2) 若 F 为域, 则 $M_n(F)$ 是单环.

(3) 设 I 是含幺交换环 R 中的理想, 求证有环同构: $M_n(R)/M_n(I) \cong M_n(R/I)$.

证 (1) 设 J 是 $M_n(R)$ 的理想, 令 I 是 J 中矩阵的矩阵元作成的集合, 则 $J \subseteq M_n(I)$. 欲证 I 是 R 的理想且 $J = M_n(I)$, 只要证对任一 $a \in I$ 和任一矩阵单位 e_{ij}, 均有 $ae_{ij} \in J$.

设 $a \in I$, 则存在 $B = \sum_{u,v} b_{uv} e_{uv} \in J$ 使得 $b_{st} = a$. 则对于任一 (i,j) 有

$$e_{is} B e_{tj} = \sum_{u,v} b_{uv} e_{is} e_{uv} e_{tj} = \sum_{u,v} b_{uv} \delta_{su} \delta_{vt} e_{ij} = a e_{ij} \in J,$$

其中 δ_{ij} 是 Kronecker 符号.

(2) 由 (1) 即得.

(3) 定义环同态 $\pi: \ M_n(R) \longrightarrow M_n(R/I)$, $\pi((a_{ij})) = (\overline{a_{ij}})$, 其中 $\overline{a_{ij}}$ 是 a_{ij} 在 R/I 中的像, 则 π 是满同态且 $\mathrm{Ker}\ \pi = M_n(I)$. 从而由环同态基本定理即知 $M_n(R/I) \cong M_n(R)/M_n(I)$. ■

2.2.5. 设 I_1 和 I_2 均是环 R 的理想, 求证:

(1) $I_1 I_2$ 也是环 R 的理想, 并且 $I_1 I_2 \subseteq I_1 \bigcap I_2$. 是否一定有 $I_1 I_2 = I_1 \bigcap I_2$?

(2) $I_1 + I_2$ 也是环 R 的理想, 并且它恰好是包含 I_1 和 I_2 的最小理想.

(3) 设 $I_1 = n\mathbb{Z}$, $I_2 = m\mathbb{Z}$ $(n, m \geqslant 1)$ 是整数环 $\mathbb{Z}$ 的两个理想, 求证: $I_1 I_2 = nm\mathbb{Z}$, $I_1 + I_2 = (n,m)\mathbb{Z}$, $I_1 \bigcap I_2 = [n,m]\mathbb{Z}$.

证 所有的结论依定义可直接验证. 一般地未必有 $I_1 I_2 = I_1 \bigcap I_2$. 例如, 若 n, m 是一对不互素的正整数, $I_1 = n\mathbb{Z}$, $I_2 = m\mathbb{Z}$, 则 $I_1 I_2 = nm\mathbb{Z} \neq [n,m]\mathbb{Z} = I_1 \bigcap I_2$. ■

2.2.6. 设 $f: R \longrightarrow S$ 是环的同态, I 和 J 分别是环 R 和 S 的理想, 并且 $f(I) \subseteq J$. 按以下方式作商环之间的映射:

$$\overline{f}: R/I \longrightarrow S/J \ \ , \ \ \overline{a} \mapsto [f(a)],$$

其中, 对于 $a \in R$, $\overline{a} = a + I$ 为 R/I 中的元, 而 $[f(a)] = f(a) + J$ 为 S/J 中的元.

(1) 说明 $\overline{f}$ 是定义合理的, 且是环同态.

(2) $\overline{f}: R/I \longrightarrow S/J$ 是环同构 $\iff$ $f(R) + J = S$ 并且 $I = f^{-1}(J)$.

证 由定义直接验证. ■

2.2.7. 设 $f: R \longrightarrow S$ 是环的同态. 如果 R 是体, 求证 f 或者是零同态, 或者是嵌入.

证 设 R 是体, 因 $\mathrm{Ker}\, f$ 是 R 的理想, 故 $\mathrm{Ker}\, f$ 或者是零, 或者是 R. 前者 f 是嵌入, 后者 f 是零同态. ■

2.2.8. 设 $(R, +, \cdot)$ 是含幺环. 对于 $a, b \in R$, 定义 $a \oplus b = a + b + 1$, $a \odot b = ab + a + b$. 求证 $(R, \oplus, \odot)$ 也是含幺环, 并且与环 $(R, +, \cdot)$ 同构.

证 直接验证 $(R, \oplus, \odot)$ 是有零元 -1 和单位元 0 的环. 考虑映射

$$\pi: \ (R, \oplus, \odot) \longrightarrow \ (R, +, \cdot), \quad a \mapsto \ a + 1.$$

则 π 是环同构. ■

2.2.9. 求证:

(1) 若 R 是主理想整环, 则 R 的每个同态像也是主理想整环.

(2) $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ $(m \geqslant 1)$ 是主理想整环.

证 直接验证 (1). 结论 (2) 是 (1) 的推论. ■

2.2.10. 环 $\mathbb{Z}/3\mathbb{Z}$ 与环 $\mathbb{Z}/6\mathbb{Z}$ 的子环 $2\mathbb{Z}/6\mathbb{Z}$ 是否同构?

证 是. 环 $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$ 的单位元是 $\overline{1}$, 环 $\mathbb{Z}/6\mathbb{Z}$ 的子环 $2\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{2}, \overline{4}\}$ 的单位元是 $\overline{4}$. 令 $f: \mathbb{Z}/3\mathbb{Z} \longrightarrow 2\mathbb{Z}/6\mathbb{Z}$, $f(\overline{0}) = \overline{0}$, $f(\overline{1}) = \overline{4}$, $f(\overline{2}) = \overline{2}$, 则 f 是环同构.

注 令 $g: \mathbb{Z}/3\mathbb{Z} \longrightarrow 2\mathbb{Z}/6\mathbb{Z}$, $g(\overline{0}) = \overline{0}$, $g(\overline{1}) = \overline{2}$, $f(\overline{2}) = \overline{4}$, 则 g 是加法群的同构, 但非环同构. ■

2.2.11. 设 $I_1, \cdots, I_n, \cdots$ 均是环 R 中的理想, 并且 $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$. 求证集合 $\bigcup\limits_{i=1}^{\infty} I_n$ 也是环 R 的理想.

证 由定义直接验证. ■

2.2.12*. 求证 $T = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z} \right\}$ 是环 $M_2(\mathbb{Z})$ 的子环; 试决定环 T 的所有理想.

证 记 $\mathbb{N}_0$ 为非负整数集, $\mathbb{N} := \mathbb{N}_0 - \{0\}$. 我们断言: 当 (q_1, q_2, l) 取遍 $\mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}$ 的元, $T(q_1, q_2, l)$ 就给出了 T 的所有两两不同的非零理想, 其中

$$T(q_1, q_2, l) = \begin{pmatrix} q_1 l\mathbb{Z} & 0 \\ l\mathbb{Z} & q_2 l\mathbb{Z} \end{pmatrix}.$$

为此, 设 I 是 T 的非零理想. 只要证 I 为上述形式.

步骤 1. 因 I 是 T 的非零理想, 故 I 中总有矩阵, 其 $(2,1)$ 处非零. 设 l 是 I 中 $(2,1)$ 处最小的正整数, 则 I 中任一矩阵的 $(2,1)$ 处均属于 $l\mathbb{Z}$.

事实上, 由 l 的选择知, 存在 $\begin{pmatrix} a & 0 \\ l & c \end{pmatrix} \in I$. 设 $0 \neq \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \in I$. 若 $y \neq 0$, 则有 $y = ql + r$, $0 \leqslant r \leqslant l - 1$. 于是

$$\begin{pmatrix} 0 & 0 \\ r & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & q \end{pmatrix} \begin{pmatrix} a & 0 \\ l & c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I$$

从而必有 $r = 0$, 即 $l \mid y$.

步骤 2. 类似地可证:

(1) 设 I 中有矩阵, 其 $(1,1)$ 处非零. 令 n 是 I 中 $(1,1)$ 处的最小正整数, 则 I 中任一矩阵 $(1,1)$ 处均属于 $n\mathbb{Z}$.

(2) 设 I 中有矩阵, 其 $(2,2)$ 处非零. 令 m 是 I 中 $(2,2)$ 处的最小正整数, 则 I 中任一矩阵 $(2,2)$ 处均属于 $m\mathbb{Z}$.

因此, $I \subseteq \begin{pmatrix} n\mathbb{Z} & 0 \\ l\mathbb{Z} & m\mathbb{Z} \end{pmatrix}$, $(n,m,l) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}$.

步骤 3. 必有 $l \mid n,\ l \mid m$.

事实上, 易知 $\begin{pmatrix} 0 & 0 \\ n & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ l & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ m & 0 \end{pmatrix} \in I$. 再由 l 的选取易推知 $l \mid n$, $l \mid m$.

因此, $I \subseteq \begin{pmatrix} n\mathbb{Z} & 0 \\ l\mathbb{Z} & m\mathbb{Z} \end{pmatrix},\ n = q_1 l,\ m = q_2 l,\ (q_1, q_2, l) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}$.

步骤 4. 最后证明 $I = T(q_1, q_2, l)$.

事实上, 由 l, m, n 的选择知, 存在 I 中的元 $\begin{pmatrix} n & 0 \\ y & z \end{pmatrix}, \begin{pmatrix} x & 0 \\ y' & m \end{pmatrix}, \begin{pmatrix} a & 0 \\ l & c \end{pmatrix}$. 因此

$$\begin{pmatrix} qn & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} q & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} n & 0 \\ y & z \end{pmatrix} \in I.$$

同理 $\begin{pmatrix} 0 & 0 \\ 0 & q'm \end{pmatrix} \in I$, $\begin{pmatrix} 0 & 0 \\ q''l & 0 \end{pmatrix} \in I$. 于是 $\begin{pmatrix} qn & 0 \\ q''l & q'm \end{pmatrix} \in I,\ \forall\, q,\ q',\ q'' \in \mathbb{Z}$.

综上所述, I 形如 $T(q_1, q_2, l)$. ■

§3　同态的应用

知识要点:

无零因子的含幺环的特征; 整环的商域; 环的直积; 中国剩余定理及其在“秘密共享”中的应用; 极大理想、素理想及其关系; 主理想整环中的极大理想与非零素理想的一致性.

2.3.1. 设 R 为无零因子环 (未必有单位元) 且满足 $pr = 0,\ \forall\, r \in R$, 其中 p 为素数. 能否将 R 嵌到一个无零因子的含幺环 S 中, 使得 S 的特征为 p?

证　可以. 令 $S = R \oplus \mathbb{Z}_p$, 按分量定义其加法, 并定义乘法如下:

$$(r_1, \overline{k}_1)(r_2, \overline{k}_2) = (r_1 r_2 + k_2 r_1 + k_1 r_2, \overline{k}_1 \overline{k}_2).$$

由于 $pr = 0,\ \forall\, r \in R$, 这个乘法的定义是合理的. 则 S 对于上述加法和乘法作成有单位元的环, 其单位元为 $(0,1)$, 并且 $f(r) = (r, 0)$ 就给出了 R 到 S 的单同态.

根据定义容易看出 S 是无零因子环. ■

2.3.2. 设 D 为整环, m 和 n 为互素的正整数, $a,b\in D$. 如果 $a^m=b^m$, $a^n=b^n$, 求证 $a=b$.

证 不妨设 $a\neq 0, b\neq 0$. 因 $(m,n)=1$, 故存在整数 s, t 使得 $ms+nt=1$. 若 $s\geqslant 0$, 则 $t\leqslant 0$. 则

$$bb^{ms}=ba^{ms}=ba^{1-nt}=ab(a^n)^{-t}=ab(b^n)^{-t}=ab^{ms},$$

从而 $a=b$. 若 $s\leqslant 0$, 同理可证. ■

2.3.3. 设 R_i $(i\in I)$ 是一个非空的环族, $R=\prod\limits_{i\in I}R_i$. 求证:

(1) R 为含幺环 $\Longleftrightarrow$ 每个 R_i 均为含幺环.

(2) R 为交换环 $\Longleftrightarrow$ 每个 R_i 均为交换环.

(3) $x=(x_i)$ 是 R 中单位 $\Longleftrightarrow$ 每个 x_i 均为 R_i 中单位.

(4) 若 R 为含幺环且 I 有限, 则 R 中理想 A 均形如 $I=\prod\limits_{i\in I}A_i$, 其中每个 A_i 是 R_i 中理想.

证 (1)—(3) 由定义可直接证明.

(4) 设 A 是 R 的理想. 令 $A_i=\{x_i\in R_i\mid$ 存在 A 中的元, 其属于 R_i 的分量为 $x_i\}$, 则 A_i 是 R_i 的理想, 且 $A\subseteq\prod\limits_{i\in I}A_i$.

设 $x=(x_i)\in\prod\limits_{i\in I}A_i$. 因 I 是有限集, 故 $x=\sum\widetilde{x_i}$, 其中 $\widetilde{x_i}$ 为第 i 个分量为 x_i, 其余分量为 0 的元. 因 $x_i\in A_i$, 故有 $a_i\in A$, a_i 的第 i 个分量为 x_i. 则 $\widetilde{x_i}=e_ia_i\in A$, 其中 e_i 为第 i 个分量为 1, 其余分量为 0 的元. 由此 $x\in A$. 这就证明了 $A=\prod\limits_{i\in I}A_i$. ■

2.3.4. 设 S, R_i $(i\in I)$ 均为环, $R=\prod\limits_{i\in I}R_i$, $\pi_i:\ R\longrightarrow R_i(i\in I)$ 为正则投射, $\varphi_i:S\longrightarrow R_i$ $(i\in I)$ 均是环的同态. 求证存在唯一的环同态 $\varphi:S\longrightarrow R$, 使得对于每个 $i\in I$, 均有 $\pi_i\varphi=\varphi_i$.

证 对任一 $s\in S$, 定义 $\varphi(s)$ 为 $\prod\limits_{i\in I}R_i$ 中的元, 其第 i 个分量为 $\varphi_i(s)$. 则 φ 满足要求. 唯一性由 $\pi_i\varphi=\varphi_i$ 即得. ■

2.3.5. 设 R_i $(i\in I)$ 均为环, 求证:

(1) $\bigoplus\limits_{i\in I}R_i=\{(x_i)\in\prod\limits_{i\in I}R_i\mid$ 只有有限多个 $x_i\neq 0\}$ 是 $\prod\limits_{i\in I}R_i$ 的子环. $\bigoplus\limits_{i\in I}R_i$ 叫做环 R_i $(i\in I)$ 的直和.

(2) 设 S 为环, 对于每个 $i\in I$, $\varphi_i:\ R_i\longrightarrow S$ 均为环同态, $\tau_i: R_i\longrightarrow \bigoplus_{i\in I} R_i$ 是正则嵌入. 则存在唯一的环同态 $\varphi:\ \bigoplus_{i\in I} R_i\longrightarrow S$, 使得 $\varphi_i=\varphi\cdot\tau_i$.

证 (1) 直接验证.

(2) 对任一 $x=(x_i)_{i\in I}\in\bigoplus_{i\in I} R_i$, 定义 $\varphi(x)=\sum_{i\in I}\varphi_i(x_i)$ (注意这是一个有限和). 则 φ 满足要求. 唯一性由 $\varphi_i=\varphi\cdot\tau_i$ 即得. ■

注 (1) 若 I 为有限集, 则由定义即知 $\bigoplus_{i\in I} I_i=\prod_{i\in I} I_i$.

(2) 题 2.3.3 的结论对于直和均成立, 其中第 (4) 小题中 I 是无限集也对.

2.3.6. 设 $I_1,\cdots,I_n$ 是环 R 的理想, 并且

(1) $I_1+\cdots+I_n=R$;

(2) 对于每个 i $(1\leqslant i\leqslant n)$, $I_i\bigcap(I_1+\cdots+I_{i-1}+I_{i+1}+\cdots+I_n)=(0)$.

求证 $R\cong\bigoplus_{i=1}^{n} I_i$.

证 首先, 由题设可知 R 中任一元均可唯一地表达成 $r=r_1+\cdots+r_n$, 其中 $r_i\in I_i$, $1\leqslant i\leqslant n$. 因此 $r\mapsto(r_1,\cdots,r_n)$ 就给出 R 到 $\bigoplus_{i=1}^{n} I_i$ 的同构. ■

2.3.7. 环 R 中元 e 叫做幂等元, 如果 $e^2=e$. 如果 e 又属于环 R 的中心, 则称 e 为中心幂等元.

设 R 是含幺环, e 为 R 的中心幂等元. 求证:

(1) $1-e$ 也是中心幂等元.

(2) eR 和 $(1-e)R$ 均是 R 的理想, 并且 $R\cong eR\times(1-e)R$.

证 由定义直接验证. ■

2.3.8. 环 R 中幂等元 e_1,e_2 称为正交的, 如果 $e_1e_2=0=e_2e_1$. 设 $R,R_1,\cdots,R_n$ 都是含幺环, 则下列两个条件等价:

(1) $R\cong R_1\times\cdots\times R_n$;

(2) R 具有两两正交的中心幂等元 $e_1,\cdots,e_n$, 使得 $e_1+\cdots+e_n=1_R$, 并且 $e_iR\cong R_i$ $(1\leqslant i\leqslant n)$.

证 由定义直接验证. ■

2.3.9*. 设 R 是含幺交换环, $P_1,\cdots,P_m$ 为 R 的素理想而 A 为 R 的理想. 如果 $A\subseteq P_1\bigcup\cdots\bigcup P_m$, 则必存在某个 i $(1\leqslant i\leqslant m)$, 使得 $A\subseteq P_i$.

证 不妨设 $P_1,\cdots,P_m$ 互不包含, 则 $\bigcap_{j\neq i}P_j\not\subseteq P_i$, $\forall i$ (否则 $P_1\cdots P_{i-1}P_{i+1}\cdots$

$P_m \subseteq \bigcap\limits_{j\neq i} P_j \subseteq P_i$. 因 P_i 是素理想, 故存在 $P_j \subseteq P_i$, $j \neq i$.). 因此存在 $r_i \in \bigcap\limits_{j\neq i} P_j$, $r_i \notin P_i$, $\forall\, i$.

假设 $A \not\subseteq P_i, \forall i$. 则存在 $a_i \in A$, $a_i \notin P_i$, $1 \leqslant i \leqslant m$. 于是 $r = \sum a_i r_i \in A \subseteq P_1 \bigcup \cdots \bigcup P_m$. 从而存在 $k, 1 \leqslant k \leqslant m$, 使 $r \in P_k$. 因为 $r_i \in P_k$, $\forall i \neq k$, 故 $a_k r_k \in P_k$. 但 P_k 是素理想, 则 $a_k \in P_k$ 或 $r_k \in P_k$. 矛盾! ■

2.3.10. 试证: 含幺交换有限环 R 的素理想 I 必是极大理想.

证 此时商环 R/I 是有限整环, 因此 R/I 是域, 从而 I 是极大理想. ■

2.3.11. 设 P 是含幺交换环 R 的素理想, $A_1, \cdots, A_n$ 是 R 的理想. 如果 $P = \bigcap\limits_{1\leqslant i\leqslant n} A_i$, 则 P 必等于某个 A_i.

证 $A_1 \cdots A_n \subseteq \bigcap\limits_{1\leqslant i\leqslant n} A_i = P$. 因 P 是素理想, 故存在 $A_i \subseteq P$. 从而 $A_i \subseteq P \subseteq A_i$, 即 $P = A_i$. ■

2.3.12. 设 $f: R \longrightarrow S$ 是环的满同态, $K = \operatorname{Ker} f$. 求证:

(1) 若 P 是 R 的素理想并且 $P \supseteq K$, 则 $f(P)$ 也是 S 的素理想.

(2) 若 Q 是 S 的素理想, 则 $f^{-1}(Q) = \{a \in R \mid f(a) \in Q\}$ 也是 R 的素理想.

(3) S 中素理想与 R 中包含 K 的素理想是一一对应的.

将素理想改成极大理想, 则以上三个论断也成立.

证 由定义直接证明. 注意到 S 的理想均形如 L/K, 其中 L 是 R 的包含 K 的理想. ■

2.3.13. 设 I 是环 R 的理想. 求证 R/I 中素理想均可写成形式 P/I, 其中 P 是 R 中素理想而且包含 I.

将素理想改成极大理想则此论断也成立.

证 R/I 的任一理想形如 P/I, 其中 P 是 R 的包含 I 的理想. 若 P/I 是素理想, 考虑标准满同态 $\pi: R \longrightarrow R/I$. 注意到 $\pi^{-1}(P/I) = P$. 由题 2.3.12(2) 知 P 是素理想.

极大理想的情形可类似证明. ■

2.3.14. 设 $m \geqslant 2$. 试决定环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 的全部素理想和极大理想.

解 $\mathbb{Z}$ 的极大理想和非零素理想同为 $p\mathbb{Z}$, p 为素数. 因此由题 2.3.13 知 $\mathbb{Z}_m$ 的素理想和极大理想为 $p\mathbb{Z}/m\mathbb{Z}$, 其中 $p \mid m$. ■

2.3.15. 设环 R 的加法群同构于有理数加法群 $(\mathbb{Q}, +)$, 而乘法则定义为 $ab = 0$, $\forall\, a, b \in R$. 求证 R 没有素理想和极大理想.

证　首先, R 的加法群的任一子群均为理想. 因为 $(\mathbb{Q},+)$ 没有极大子群, 故 R 没有极大理想. 设 I 是 R 的任一理想且 $I \neq R$, 则 $R^2 = 0 \subseteq I$. 这表明 R 无素理想. ■

2.3.16. (1) 设 R 是含幺环, 则 R 的极大理想均为素理想.

(2) 设 R 是主理想整环, 则 R 的任一非零素理想均为极大理想.

(3) 设 F 为域, 试问 $F[x]$ 中哪些理想是素理想和极大理想?

证　(1) 否则, 设 M 是 R 的极大理想且非素理想, 则存在 R 的理想 A 和 B 使得 $A \not\subseteq M$, $B \not\subseteq M$, $AB \subseteq M$. 于是 $R = A + M = B + M$, 从而 $R = R^2 = (A+M)(B+M) \subseteq AB + M \subseteq M$. 与 $M \neq R$ 相矛盾.

(2) 设 $P = \langle p \rangle$ 是 R 的非零素理想. 若 $P \subsetneqq \langle a \rangle$, 则 $a \mid p$, 即 $p = ab, b \in R$. 令 $A = \langle a \rangle$, $B = \langle b \rangle$, 则 $AB = \langle ab \rangle = \langle p \rangle = P$. 由 P 是素理想知 $B \subseteq P$, 即 $p \mid b$, 即 $b = pc, c \in R$. 于是

$$p = acp \ , \ ac = 1,$$

即 $\langle a \rangle = R$. 这就证明了 P 是极大理想.

(3) 因 $F[x]$ 是主理想整环, 故由 (1) 和 (2) 易知 $F[x]$ 的极大理想恰是 $\langle p(x) \rangle$, 其中 $p(x)$ 是 $F[x]$ 中的不可约多项式.

而 $F[x]$ 的素理想为零理想, 或 $\langle p(x) \rangle$, 其中 $p(x)$ 是 $F[x]$ 中的不可约多项式. ■

2.3.17. 试证: 有单位元的非零环 R 的任一真理想必包含于某一极大理想. 特别地, R 有极大理想 (从而有素理想).

证　设 I 是 R 的真理想, 令 S 是 R 的包含 I 的真理想的集合, 则 S 非空 (起码 I 在 S 中), 则 S 对于通常的包含关系 $\subseteq$ 作成一个偏序集. 设 T 是 S 的一个链, 则 $\bigcup\limits_{J \in T} J$ 也是 R 的不含 1 的包含 I 的理想, 因此它是这个链的一个上界. 从而由 Zorn 引理知 S 有极大元 M, 这个极大元就是 R 的一个极大理想, 并且包含 I.

因为零理想是 R 的真理想, 故由上述结论即知 R 有极大理想. ■

§4　各 类 整 环

知识要点:

不可约元与素元及其关系; 唯一因子分解整环 (UFD) 的定义; 非 UFD 的例子; UFD 的等价刻画; 主理想整环 (PID) 和 Euclid 整环 (ED).

域是 ED; ED 是 PID; PID 是 UFD; UFD 当然是整环. 这些结论的逆均不成立.

2.4.1. (1) 设 R 为整环. 若 $\langle p\rangle$ 是 R 的非零极大理想, 则 p 为不可约元.

(2) 设 R 为主理想整环. 若 p 为不可约元, 则 $\langle p\rangle$ 也是 R 的极大理想.

证 (1) 首先, 易知 $p\neq 0$, $p\notin U(R)$. 设 c 是 p 的因子, 则 $\langle c\rangle\supseteq\langle p\rangle$. 因 $\langle p\rangle$ 是 R 的极大理想, 故 $\langle c\rangle=\langle p\rangle$ 或者 $\langle c\rangle=R$, 从而 c 与 p 相伴或者 c 是单位.

(2) 设 p 为不可约元, 则 $\langle p\rangle\neq R$. 设 I 是包含 $\langle p\rangle$ 的 R 的理想且 $I\neq\langle p\rangle$. 因 R 为主理想整环, 故有 $c\in R$ 使得 $I=\langle c\rangle\supseteq\langle p\rangle$. 于是有 $d\in R$ 使得 $p=cd$. 因 $I\neq\langle p\rangle$, 故 c 不与 p 相伴. 从而 c 是单位, 即 $I=R$. 这就证明了 $\langle p\rangle$ 是 R 的极大理想. ■

2.4.2. 设 R 为整环, 则 p 为素元当且仅当 $\langle p\rangle$ 是 R 的非零素理想.

证 设 p 为素元, 则 $0\neq\langle p\rangle\neq R$. 设 I 和 J 是 R 的理想且 $IJ\subseteq\langle p\rangle$. 若 $I\nsubseteq\langle p\rangle$, $J\nsubseteq\langle p\rangle$, 则有 $a\notin\langle p\rangle$, $a\in I$ 和 $b\notin\langle p\rangle$, $b\in J$, 使得 $ab\in\langle p\rangle$, 于是 $p\mid ab$. 因 p 为素元, 故 $p\mid a$ 或 $p\mid b$. 这与 $a\notin\langle p\rangle$, $b\notin\langle p\rangle$ 相矛盾. 这就证明了 $\langle p\rangle$ 是 R 的素理想.

反之, 设 $\langle p\rangle$ 是 R 的非零素理想, 则 $p\neq 0$, $p\notin U(R)$. 设 $p\mid ab$, 则 $\langle a\rangle\langle b\rangle=\langle ab\rangle\subseteq\langle p\rangle$. 因 $\langle p\rangle$ 是 R 的素理想, 故 $\langle a\rangle\subseteq\langle p\rangle$ 或者 $\langle b\rangle\subseteq\langle p\rangle$, 即 $p\mid a$ 或者 $p\mid b$. ■

2.4.3. (1) 设 R 为整环. 若 p 为素元, 则 p 为不可约元.

(2) 设 R 为主理想整环. 若 p 为不可约元, 则 p 为素元.

证 (1) 若 p 为素元, 设 $p=ab$, 则 $p\mid ab$. 故 $p\mid a$ 或 $p\mid b$. 若 $p\mid a$, 则有 $c\in R$ 使得 $a=pc$, 于是 $p=pcb$, 即 b 是单位. 同理, 若 $p\mid b$, 则 a 是单位. 这就证明了 p 是不可约元.

(2) 此时, 由题 2.4.1(2) 知 $\langle p\rangle$ 是 R 的极大理想, 从而是 (非零) 素理想 (参见题 2.3.16(1)). 再由题 2.4.2 知 p 为素元.

以下给出这个结论的一个直接证明.

若 p 为不可约元, 设 $p\mid ab$, $p\nmid a$. 由题 2.4.1(2) 知 $\langle p\rangle$ 是 R 的极大理想, 因此 $\langle p\rangle+\langle a\rangle=R$. 于是有 $c,d\in R$ 使得 $1=pc+ad$, 从而 $b=pcb+abd$. 由此可见 $p\mid b$. ■

2.4.4. 设 a 为主理想整环 D 中的非零元. 求证: 若 a 为素元, 则 $D/\langle a\rangle$ 为域; 若 a 不是素元, 则 $D/\langle a\rangle$ 不是整环.

证 若 a 为素元, 则 $\langle a\rangle$ 是素理想, 从而 $\langle a\rangle$ 是极大理想 (参见题 2.3.16(2)), 进而 $D/\langle a\rangle$ 为域.

若 a 不是素元, 则 $\langle a\rangle$ 不是素理想, 从而 $D/\langle a\rangle$ 有零因子. ■

2.4.5. 设 R 为整环, $a, b \in R-\{0\}$, $a \sim b$ (即 a 与 b 相伴). 求证:

(1) 若 a 为不可约元, 则 b 也为不可约元.

(2) 若 a 为素元, 则 b 也为素元.

证 由定义直接证明. ■

2.4.6. 设 R 为 UFD, a, b, c 为 R 中非零元. 求证:

(1) $ab \sim (a,b)[a,b]$;

(2) 若 $a \mid bc$, $(a,b)=1$, 则 $a \mid c$.

证 由定义直接证明. ■

2.4.7. 设 R 为 PID, 求证:

(1) $\langle a\rangle \bigcap \langle b\rangle = \langle [a,b]\rangle$; 并且 $\langle a\rangle \bigcap \langle b\rangle = \langle a\rangle\langle b\rangle \Longleftrightarrow (a,b)=1$.

(2) 方程 $ax+by=c$ 在 R 中有解 (x,y) 的充分条件是 $(a,b) \mid c$.

证 由定义直接证明. ■

2.4.8. 如果 D 为整环但不是域, 则 $D[x]$ 不是主理想整环. 特别地, $\mathbb{Z}[x]$ 不是 PID.

证 设 d 是 D 中非零的不可逆元, 则 $\langle d,x\rangle$ 不是主理想. 否则, 设 $\langle d,x\rangle = \langle f(x)\rangle$. 则由 $d \in \langle f(x)\rangle$ 可知 $f(x)$ 是零次多项式, 记为 c. 于是

$$\langle d,x\rangle = \langle c\rangle,\ c \in D.$$

再由 $x \in \langle c\rangle$ 可知 c 是 D 中可逆元, 从而 $\langle d,x\rangle = D[x]$. 于是存在 $g(x), h(x) \in D[x]$, 使得

$$1 = dg(x) + xh(x).$$

因此 $1 = dg_0$, 其中 g_0 是 $g(x)$ 的常数项. 这与 d 不可逆相矛盾! ■

2.4.9. 证明 $\mathbb{Z}[\sqrt{-2}\,]$ 是 ED, 从而是 UFD. 而 $\mathbb{Z}[\sqrt{-3}\,]$ 不是 UFD.

证 定义映射 $\varphi : \mathbb{Z}[\sqrt{-2}\,] \longrightarrow \mathbb{N}_0$ 为 $\varphi(a+b\sqrt{-2}) = a^2+2b^2$. 则 $\varphi(\alpha)=0$ 当且仅当 $\alpha=0$; $\varphi(\alpha\beta)=\varphi(\alpha)\varphi(\beta)$, $\forall\ \alpha,\ \beta \in \mathbb{Z}[\sqrt{-2}\,]$. 设 $\alpha,\ 0 \neq \beta \in \mathbb{Z}[\sqrt{-2}\,]$. 令 $\alpha\beta^{-1} = x+y\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}\,]$. 取 $a, b \in \mathbb{Z}$ 使得 $c = x-a$ 和 $d = y-b$ 满足 $|c| \leqslant \dfrac{1}{2}$, $|d| \leqslant \dfrac{1}{2}$. 于是有

$$\alpha = (a+b\sqrt{-2})\beta + r,$$

其中 $r = (c+d\sqrt{-2})\beta \in \mathbb{Z}[\sqrt{-2}\,]$, 并且

$$\varphi(r) = \varphi(c+d\sqrt{-2})\varphi(\beta) = (c^2+2d^2)\varphi(\beta) \leqslant \left(\frac{1}{4}+\frac{2}{4}\right)\varphi(\beta) < \varphi(\beta).$$

由定义知 $\mathbb{Z}[\sqrt{-2}\,]$ 是 ED.

注意 $\mathbb{Z}[\sqrt{-3}\,]$ 中的单位恰为 ± 1. 在 $\mathbb{Z}[\sqrt{-3}\,]$ 中有如下两种不可约分解:

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3}),$$

其中 2, $1\pm\sqrt{-3}$ 均为 $\mathbb{Z}[\sqrt{-3}\,]$ 中的素元. 因为 2 与 $1\pm\sqrt{-3}$ 在 $\mathbb{Z}[\sqrt{-3}\,]$ 中不相伴, 故由定义知 $\mathbb{Z}[\sqrt{-3}\,]$ 不是 UFD. ■

2.4.10. 设 D 是 PID, E 为整环, 并且 D 是 E 的子环, $a,b \in D-\{0\}$. 如果 d 是 a 和 b 在 D 中的最大公因子, 证明 d 也是 a 和 b 在 E 中的最大公因子.

证　因为 D 是 PID, 则存在 $x,y \in D$ 使得 $d = ax+by$. 设 d' 是 a 和 b 的公因子且 $d' \in E$, 则 $d' \mid d$. 由此即知 d 也是 a, b 在 E 中的最大公因子. ■

2.4.11. 求 50 和 $19+9\mathrm{i}$ 在 $\mathbb{Z}[\mathrm{i}]$ 中的最大公因子.

解　因 $\mathbb{Z}[\mathrm{i}]$ 是 Euclid 整环, 故其中两个元的最大公因子可用辗转相除法求得. 令 $\varphi(a+b\mathrm{i}) = a^2+b^2$, 我们有

$$\begin{aligned}
50 &= (2-\mathrm{i})(19+9\mathrm{i})+3+\mathrm{i}, && \varphi(3+\mathrm{i}) < \varphi(19+9\mathrm{i}),\\
19+9\mathrm{i} &= (6+\mathrm{i})(3+\mathrm{i})+2, && \varphi(2) < \varphi(3+\mathrm{i}),\\
3+\mathrm{i} &= 2+(1+\mathrm{i}), && \varphi(1+\mathrm{i}) < \varphi(2),\\
2 &= (1-\mathrm{i})(1+\mathrm{i}).
\end{aligned}$$

所以 $(50, 19+9\mathrm{i}) = 1+\mathrm{i}$. ■

2.4.12*. 设 $a+b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, 且 $a^2+b^2 = p$, p 为素数, 则 $\mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle \cong \mathbb{Z}_p$.

证　因 $(a,b)=1$, 故有整数 l,k, 使得 $al+bk=1$. 于是 $(a+b\mathrm{i})(k+l\mathrm{i}) = (ak-bl)+\mathrm{i}$. 这表明在 $\mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle$ 中 $\bar{\mathrm{i}} = \bar{r}$, 其中 $r \in \mathbb{Z}$. 又因 $\bar{p} = 0$, 故 $\mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle = \{\,\bar{0},\cdots,\overline{p-1}\}$. 由此易知 $\mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle \cong \mathbb{Z}_p$. ■

§5　多 项 式 环

知识要点:

虽然可以讨论一般环上的多项式环, 但以下主要关心整环上的多项式环.

域上多项式的重根的判定; Eisenstein 不可约性判别法; Gauss 定理: UFD 上的多项式环仍是 UFD; 域上一元多项式环是 ED; 域上多元多项式环不是主理想整环.

2.5.1. 试决定环 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 的自同构群.

证　$\forall \sigma \in \mathrm{Aut}(\mathbb{Z}[x])$, 因 $\sigma(1)=1$, 可推出 $\sigma|_{\mathbb{Z}} = \mathrm{id}$. 令 $\sigma(x) \in \mathbb{Z}[x]$ 的次数为 n. 因 σ 是自同构, 故存在 $g(x) \in \mathbb{Z}[x]$ 使得 $x = \sigma(g(x)) = g(\sigma(x))$, 这迫使 $n=1$.

设 $\sigma(x)=ax+b$, $g(x)=cx+d$. 于是 $x=c(ax+b)+d=cax+cb+d$. 故 $ca=1$, 从而 $a=\pm1$. 于是 $\sigma(f(x))=f(ax+b)$, $\forall f(x)\in\mathbb{Z}[x]$.

反之, 给定任一 (a,b), 其中 $a=\pm1$, $b\in\mathbb{Z}$. 则 $\sigma_{(a,b)}:\ f(x)\mapsto f(ax+b)$ 是 $\mathbb{Z}[x]$ 的环自同构.

令

$$\psi:\ \mathrm{Aut}(\mathbb{Z}[x])\longrightarrow\left\{\begin{pmatrix}a&0\\b&1\end{pmatrix}\in M_2(\mathbb{Z})\ \middle|\ a=\pm1,\ b\in\mathbb{Z}\right\},$$

$$\sigma_{(a,b)}\ \mapsto\ \begin{pmatrix}a&0\\b&1\end{pmatrix},$$

下证 ψ 是群同构. 首先 ψ 是定义合理的: 若 $\sigma_{(a,b)}=\sigma_{(c,d)}$ 则 $\sigma_{(a,b)}(x)=\sigma_{(c,d)}(x)$. 即 $ax+b=cx+d$, 从而 $a=c$, $b=d$. 易证 ψ 是双射和群同态, 从而是同构. 因此

$$\mathrm{Aut}(\mathbb{Z}[x])=\left\{\begin{pmatrix}a&0\\b&1\end{pmatrix}\ \middle|\ a=\pm1,\ b\in\mathbb{Z}\right\}.$$

类似地可证 $\mathrm{Aut}(\mathbb{Q}[x])=\left\{\begin{pmatrix}a&0\\b&1\end{pmatrix}\ \middle|\ a\in\mathbb{Q}^*,\ b\in\mathbb{Q}\right\}$. ■

2.5.2. 如果 $c_0,\cdots,c_n$ 是整环 D 中两两相异的 $n+1$ 个元, $d_0,\cdots,d_n$ 是 D 中任意 $n+1$ 个元, 求证:

(1) 在 $D[x]$ 中至多存在一个次数 $\leqslant n$ 的多项式 $f(x)$, 使得 $f(c_i)=d_i$ $(0\leqslant i\leqslant n)$.

(2) 如果 D 为域, 则 (1) 中所述的多项式是存在的.

证 (1) 换言之, 我们要证明: 若有一个次数 $\leqslant n$ 的多项式 $f(x)$ 使得 $f(c_i)=0$, $\forall\ 0\leqslant i\leqslant n$, 则 $f(x)=0$.

设 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$ 具有这种性质, 则

$$\begin{pmatrix}1&c_0&c_0^2&\cdots&c_0^n\\1&c_1&c_1^2&\cdots&c_1^n\\\vdots&\vdots&\vdots&&\vdots\\1&c_n&c_n^2&\cdots&c_n^n\end{pmatrix}\begin{pmatrix}a_0\\a_1\\\vdots\\a_n\end{pmatrix}=0.$$

用 A 代表这个系数矩阵, 则 A 是 Vandermonde 矩阵. 用 $|A|$ 表示 A 的行列式, 因 $c_0,\cdots,c_n$ 两两相异, 故 $|A|\neq0$. 令 A^* 是 A 的伴随矩阵, 则 $A^*A=\mathrm{diag}\{|A|,|A|,\cdots,|A|\}$, 于是

$$|A|a_i=0,\quad a_i=0,\ 0\leqslant i\leqslant n.$$

从而 $(a_0, a_1, \cdots, a_n) = 0$, $f(x) = 0$.

(2) 由 (1) 的证明知, 若 D 是域, 则必存在唯一的次数不大于 n 的多项式 $f(x)$, 使得 $f(c_i) = d_i$, $i = 0, 1, \cdots, n$. 事实上, 令 $f(x) = \sum_{i=0}^{n} a_i x^i$, 其中 $a_i = \dfrac{d_i'}{|A|}$,

$$\begin{pmatrix} d_0' \\ d_1' \\ \vdots \\ d_n' \end{pmatrix} := A^* \begin{pmatrix} d_0 \\ d_1 \\ \vdots \\ d_n \end{pmatrix},$$

则 $f(x)$ 就是这样的多项式. ■

2.5.3. $2x+2$ 在 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 中是否为不可约元? x^2+1 在 $\mathbb{R}[x]$ 和 $\mathbb{C}[x]$ 中是否为不可约元?

证 在 $\mathbb{Z}[x]$ 中, $2x+2 = 2(x+1)$, 且 2 与 $x+1$ 均不是 $\mathbb{Z}[x]$ 中的单位, 故 $2x+2$ 在 $\mathbb{Z}[x]$ 中可约. 但 $2x+2$ 在 $\mathbb{Q}[x]$ 中不可约. x^2+1 是 $\mathbb{R}[x]$ 中不可约元, 但在 $\mathbb{C}[x]$ 中可约. ■

2.5.4. 设 D 和 E 为整环, $D \subseteq E$, $f(x) \in D[x]$, c 是 $f(x)$ 在 E 中的一个根. 利用形式微商确定根 c 的重数.

证 c 是 $f(x)$ 的 $m(m \geqslant 1)$ 重根, 当且仅当 $f(x)$ 的 $m-1$ 次形式微商 $f^{(m-1)}(x)$ 有根 c 且 m 次微商 $f^{(m)}(x)$ 不以 c 为根. ■

2.5.5. 设 F 是域, $f(x) \in F[x]$, $c_1, \cdots, c_m$ 是 $f(x)$ 在 F 中两两相异的根, 并且根 c_i 的重数为 $\lambda_i, i = 1, \cdots, m$. 求证 $\lambda_1 + \cdots + \lambda_m \leqslant \deg f$.

证 此时 $f(x) = \prod_{i=1}^{m} (x - c_i)^{\lambda_i} \cdot g(x)$, 由此即得. ■

2.5.6. 设 $f = \sum u_i x^i \in \mathbb{Z}[x]$ 为首 1 多项式, p 为素数, 以 $\overline{a}$ 表示 $a \in \mathbb{Z}$ 在环的自然同态 $\mathbb{Z} \longrightarrow \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 之下的像, 而令 $\overline{f}(x) = \sum \overline{u}_i x^i \in \mathbb{Z}_p[x]$. 求证:

(1) 如果对某个素数 p, $\overline{f}(x)$ 在 $\mathbb{Z}_p[x]$ 中不可约, 则 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约.

(2) 如果 $f(x)$ 不是 $\mathbb{Z}[x]$ 中首 1 多项式, 试问 (1) 中的结论是否成立?

证 (1) 若在 $\mathbb{Z}[x]$ 中 $f(x) = g(x)h(x)$, 其中 $\deg g, \deg h \geqslant 1$, 则在 $\mathbb{Z}_p[x]$ 中 $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$. 但 $\overline{f}(x)$ 在 $\mathbb{Z}_p[x]$ 中不可约, 唯一的可能是 $\deg \overline{g}$ 或 $\deg \overline{h} = 0$. 不妨设 $\deg \overline{g} = 0$, 因此 $g(x)$ 的首项系数是 p 的倍数. 从而 $f(x)$ 的首项系数是 p 的倍数, 这与 $f(x)$ 首 1 相矛盾.

(2) 否. 例如 $f(x) = 2x^3 - 7x^2 + x + 1 \in \mathbb{Z}[x]$. 在 $\mathbb{Z}_2[x]$ 中 $\overline{f}(x) = x^2 + x + 1$ 不可约, 但 $f(x)$ 在 $\mathbb{Z}[x]$ 中有分解 $f(x) = (2x-1)(x^2 - 3x - 1)$. ■

注 上述 (1) 给出了 $\mathbb{Z}[x]$ 中首 1 多项式不可约性的一个充分条件.

2.5.7. 设 D 为 UFD, F 为 D 的商域, $f(x)$ 为 $D[x]$ 中首 1 多项式. 求证: $f(x)$ 在 $F[x]$ 中的每个首 1 多项式因子必然属于 $D[x]$.

证 设在 $F[x]$ 中有 $f(x)=g(x)h(x)$, 其中 $g(x)$, $h(x)\in F[x]$ 且均为首 1 的. 将 $g(x)$ 和 $h(x)$ 分别写成

$$g(x)=\frac{\widetilde{g}(x)}{d_1},\quad h(x)=\frac{\widetilde{h}(x)}{d_2},\quad \widetilde{g}(x),\ \widetilde{h}(x)\in D[x],\quad d_1,\ d_2\in D.$$

于是 $d_1d_2f(x)=\widetilde{g}(x)\widetilde{h}(x)$. 因 $f(x)$ 首 1, 故 $C(d_1d_2f(x))=d_1d_2$, 由 Gauss 引理知 $d_1d_2=C(\widetilde{g}(x))C(\widetilde{h}(x))$, 其中 $C(f(x))$ 表示 $f(x)$ 的容量, 即 $f(x)$ 的各项系数的最大公因子. 因 $\widetilde{g}(x)$ 的首项系数为 d_1, $\widetilde{h}(x)$ 的首项系数为 d_2, 从而

$$C(\widetilde{g}(x))\mid d_1,\quad C(\widetilde{h}(x))\mid d_2.$$

设 $d_1=C(\widetilde{g}(x))s$, $d_2=C(\widetilde{h}(x))t$, 其中 $s,t\in D$. 于是 $stC(\widetilde{g}(x))C(\widetilde{h}(x))=C(\widetilde{g}(x))C(\widetilde{h}(x))$, 即 $st=1$. 即 $C(\widetilde{g}(x))$ 与 d_1 相伴, $C(\widetilde{h}(x))$ 与 d_2 相伴. 从而 $g(x)$, $h(x)\in D[x]$. ■

2.5.8. 设 R 是含幺交换环, $f(x)=\sum\limits_{i=0}^{n}a_ix^i\in R[x]$. 则 $f\in U(R[x])\Longleftrightarrow a_0\in U(R)$, 并且 $a_1,\cdots,a_n$ 均是 $R[x]$ 中的幂零元.

证 设 $a_0\in U(R)$, $a_1,\cdots,a_n$ 均为 $R[x]$ 中的幂零元. 则 a_ix^i 均为 $R[x]$ 中的幂零元, $i=1,\cdots,n$. 从而 $g(x)=\sum\limits_{i=1}^{n}a_ix^i$ 为 $R[x]$ 中的幂零元, 即存在 $t\geqslant 1$ 使得 $g^t(x)=0$. 于是

$$\begin{aligned}&\frac{1}{a_0^t}(a_0+g(x))(a_0^{t-1}-a_0^{t-2}g(x)+\cdots+(-1)^{t-1}g^{t-1}(x))\\&=(a_0^{-1})^t(a_0^t+(-1)^{t-1}g^t(x))\\&=1,\end{aligned}$$

即 $f(x)=a_0+g(x)\in U(R[x])$.

反之, 设 $f(x)=a_0+a_1x+\cdots+a_nx^n\in U(R[x])$. 要证 $a_0\in U(R)$, $a_1,\cdots,a_n$ 均为 $R[x]$ 中的幂零元. 对 n 用数学归纳法. 易知 $n=0$ 时成立. 设结论对次数小于 n 的多项式都成立. 由 $f(x)\in U(R[x])$ 知, 存在 $g(x)=\sum\limits_{i=1}^{m}b_ix^i$ 使得

$f(x)g(x)=1$. 于是 $a_0, b_0 \in U(R)$. 比较 x^{n+j} 的系数有:

$$\begin{aligned}
&a_n b_m = 0,\\
&a_n b_{m-1} + a_{n-1} b_m = 0,\\
&\cdots\\
&a_n b_j + a_{n-1} b_{j+1} + \cdots + a_{n-m+j} b_m = 0, \quad j \geqslant 0, \quad j \leqslant n, \ m.
\end{aligned}$$

将第二式乘以 a_n 得到 $a_n^2 b_{m-1}=0$, 再将第三式乘以 a_n 得到 $a_n^3 b_{m-2}=0$, 继续下去, 最后将最后一式乘以 a_n 得到 $a_n^{m-j} b_j = 0$. 于是 $a_n^m b_0 = 0$. 但 $b_0 \in U(R)$, 故 $a_n^m = 0$. 于是 $(a_n x^n)^m = 0$. 令 $a_n x^n = c$, 则 $c^m = 0$. 于是

$$(f(x)-c)\sum_{i=0}^{m-1} f^i(x) c^{m-i} \frac{1}{f^m(x)} = \frac{1}{f^m(x)}(f^m(x)-c^m) = 1,$$

即 $n-1$ 次多项式 $f(x)-c = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in U(R[x])$. 从而由归纳假设知 $a_1, \cdots, a_{n-1}$ 均幂零. ■

2.5.9*. (Eisenstein 判别法的推广） 设 $f(x)=\sum\limits_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, $\deg f = n$, $(a_0, a_1, \cdots, a_n) = 1$. 如果存在素数 p 和整数 k $(0 < k \leqslant n)$, 使得

$$p \nmid a_k, \quad p \mid a_i \quad (0 \leqslant i \leqslant k-1), \quad p^2 \nmid a_0,$$

求证 $f(x)$ 在 $\mathbb{Z}[x]$ 中必存在次数 $\geqslant k$ 的不可约因子.

在做本题之前, 对 Eisenstein 判别法给出一个注记 (虽然以下证明无需这个注记). Eisenstein 判别法有两种等价的表述.

定理: 设 D 为 UFD, $f(x)=\sum\limits_{i=0}^{n} a_i x^i$ 是 $D[x]$ 中 n 次本原多项式 (此处本原是指 $a_0, \cdots, a_n$ 的最大公因子为 1). 若存在 D 中的不可约元 p 使得

$$p \mid a_0, \quad p \mid a_1, \quad \cdots, \quad p \mid a_{n-1}, \quad p^2 \nmid a_0,$$

则 $f(x)$ 为 $D[x]$ 中不可约多项式 (从而也是 $F[x]$ 中不可约多项式, F 为 D 的商域).

这个表述与教材中相同: 未加假设 $p \nmid a_n$ 是因为这可从 $f(x)$ 的本原性中推出.

定理: 设 D 为 UFD, $f(x)=\sum\limits_{i=0}^{n} a_i x^i$ 是 $D[x]$ 中 n 次多项式. 若存在 D 中的不可约元 p 使得

$$p \mid a_0, \quad p \mid a_1, \quad \cdots, \quad p \mid a_{n-1}, \quad p \nmid a_n, \quad p^2 \nmid a_0,$$

则 $f(x)$ 为 $F[x]$ 中不可约多项式, F 为 D 的商域.

这个表述中未加本原性的假设, 而加上 $p \nmid a_n$. 因此 $f(x)$ 在 $D[x]$ 有可能可约.

例如 $f(x)=10x^5-30x^3+45x^2-15\in\mathbb{Z}[x]$, 取 $p=3$, 则 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约. 但 $f(x)=5(2x^5-6x^3+9x^2-3)$ 在 $\mathbb{Z}[x]$ 中可约.

证 对 n 用数学归纳法. $n=1$ 时结论显然成立. 假设结论对于满足条件的 r 次多项式 $f(x)$ 成立, 其中 $r<n$.

若 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约, 则 $f(x)$ 自身就是 $f(x)$ 的次数 $n\geqslant k$ 的不可约因子. 故以下设 $f(x)$ 在 $\mathbb{Z}[x]$ 中可约, $f(x)=g(x)h(x)$. 因为 $(a_0,a_1,\cdots,a_n)=1$, 故 $\deg g(x),\deg h(x)\neq 0$. 设 $g(x)=b_0+b_1x+\cdots+b_rx^r$, $b_r\neq 0$, $h(x)=c_0+c_1x+\cdots+c_sx^s$, $c_s\neq 0$, 则 $r,\ s\geqslant 1$, $r+s=n$. 因为 $a_0=b_0c_0$, $p\mid a_0$, 故 $p\mid b_0$ 或 $p\mid c_0$. 不妨设 $p\mid b_0$, 则 $p\nmid c_0$ 且 $p^2\nmid b_0$ (这是因为 $p^2\nmid a_0$). 因 $(a_0,a_1,\cdots,a_n)=1$, 故 $(b_0,b_1,\cdots,b_r)=1$. 于是存在正整数 t, $t\leqslant r$, 使得

$$p\mid b_i\quad(0\leqslant i\leqslant t-1),\quad p\nmid b_t.$$

若 $t<k$ 且 $t\leqslant s$, 则

$$a_t=b_tc_0+b_{t-1}c_1+\cdots+b_1c_{t-1}+b_0c_t.$$

因 $p\mid a_t$, $p\mid b_i$ $(0\leqslant i\leqslant t-1)$, 故 $p\mid b_tc_0$. 但 $p\nmid b_t$, $p\nmid c_0$, 矛盾.

若 $t<k$ 且 $t>s$, 则

$$a_t=b_tc_0+b_{t-1}c_1+\cdots+b_{t-s}c_s.$$

同理得到矛盾.

若 $t>k$ 且 $k\leqslant s$, 则

$$a_k=b_0c_k+b_1c_{k-1}+\cdots+b_{k-1}c_1+b_kc_0.$$

因 $p\mid b_i$ $(0\leqslant i\leqslant k)$, 故 $p\mid a_k$. 与 $p\nmid a_k$ 的题设相矛盾.

若 $t>k$ 且 $k>s$, 则

$$a_k=b_kc_0+b_{k-1}c_1+\cdots+b_{k-s}c_s.$$

同理得到矛盾.

因此只能 $t=k$. 即有 r 次 $(r<n)$ 多项式 $g(x)=b_0+b_1x+\cdots+b_rx^r\in\mathbb{Z}[x]$, $(b_0,b_1,\cdots,b_r)=1$, $p\mid b_i$ $(0\leqslant i\leqslant k-1)$, $p\nmid b_k$, $p^2\nmid b_0$. 由归纳假设即知, $g(x)$ 在 $\mathbb{Z}[x]$ 中存在次数 $\geqslant k$ 的不可约因子. 从而结论得证. ■

2.5.10. 将 x^n-1 $(3\leqslant n\leqslant 10)$ 在 $\mathbb{Z}[x]$ 中作素因子分解.

解 $x^3-1=(x-1)(x^2+x+1)$

$$x^4-1=(x-1)(x+1)(x^2+1),$$
$$x^5-1=(x-1)(x^4+x^3+x^2+x+1),$$
$$x^6-1=(x-1)(x+1)(x^2+x+1)(x^2-x+1),$$
$$x^7-1=(x-1)(x^6+x^5+x^4+x^3+x^2+x+1),$$
$$x^8-1=(x-1)(x+1)(x^2+1)(x^4+1),$$
$$x^9-1=(x-1)(x^2+x+1)(x^6+x^3+1),$$
$$x^{10}-1=(x-1)(x+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1).$$

■

注 (1) 令 $f(x)=x^4-x^3+x^2-x+1$, 则 $f(-x)=x^4+x^3+x^2+x+1$. 因 $f(-x)$ 在 $\mathbb{Q}[x]$ 中不可约 (应用 Eisenstein 判别法), 故 $f(x)$ 不可约.

(2) x^6+x^3+1 是分圆多项式, 因此在 $\mathbb{Z}[x]$ 上不可约. 关于分圆多项式在 $\mathbb{Z}[x]$ 上不可约的证明可参见 [FY], p.144.

2.5.11. 设 D 为整环, $f(x)\in D[x]$, $c\in D$, $g(x)=f(x+c)\in D[x]$. 求证:

(1) $f(x)$ 在 $D[x]$ 中本原 $\Longleftrightarrow g(x)$ 在 $D[x]$ 中本原.

(2) $f(x)$ 在 $D[x]$ 中不可约 $\Longleftrightarrow g(x)$ 在 $D[x]$ 中不可约.

证 (1) 设 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$, 因 $g(x)=f(x+c)$, 则 $g(x)=b_0+b_1x+b_2x^2+\cdots+b_nx^n$, 其中 $b_j=a_j+\binom{j+1}{j}a_{j+1}c+\cdots+\binom{n}{j}a_nc^{n-j}$, $j=0,1,\cdots,n$. 特别地, $b_n=a_n$. 设 $d=(b_0,b_1,\cdots,b_n)$, 则 $d\mid a_n$. 又 $d\mid a_n$, $d\mid b_{n-1}$, 则 $d\mid a_{n-1}$. 以此类推, 便可得 $d\mid a_0$. 从而 $d\mid a_0,a_1,\cdots,a_n$, 即 $(b_0,b_1,\cdots,b_n)\mid(a_0,a_1,\cdots,a_n)$. 又 $f(x)=g(x-c)$, 故 $(a_0,a_1,\cdots,a_n)\mid(b_0,b_1,\cdots,b_n)$. 于是 $(a_0,a_1,\cdots,a_n)\sim(b_0,b_1,\cdots,b_n)$. 从而得证.

(2) 易证. ■

2.5.12. 设 R 为任意环, 定义集合

$$R[[x]]=\left\{\sum_{n=0}^{\infty}a_nx^n\mid a_n\in R,\ n=0,1,2,\cdots\right\},$$

每个元 $\sum\limits_{n=0}^{\infty}a_nx^n$ 叫做 R 上关于 x 的形式幂级数. 定义

$$\sum a_nx^n+\sum b_nx^n=\sum(a_n+b_n)x^n,$$
$$\left(\sum a_nx^n\right)\left(\sum b_nx^n\right)=\sum c_nx^n,$$

其中 $c_n = \sum_{i+j=n} a_i b_j$, $n = 0, 1, 2, \cdots$. 求证:

(1) $R[[x]]$ 对于上述加法和乘法形成环, 叫做环 R 上关于 x 的形式幂级数环.

(2) 若 R 有幺元 1, 则 1 也是 $R[[x]]$ 的幺元. 若 R 为交换环, 则 $R[[x]]$ 也是交换环.

(3) 多项式环 $R[x]$ 自然看成是 $R[[x]]$ 的子环.

(4) 设 R 是含幺交换环, $f(x) = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$. 则

$$f(x) \in U(R[[x]]) \Longleftrightarrow a_0 \in U(R).$$

(5) 若 a_0 在 R 中不可约, 则 $f(x)$ 在 $R[[x]]$ 中不可约.

证 (1)—(3) 直接验证.

(4) 设 $f(x) = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$. 若 $f(x) \in U(R[[x]])$, 则显然 $a_0 \in U(R)$. 反之, 设 $a_0 \in U(R)$. 令 $g(x) = \sum_{n=0}^{\infty} b_n x^n$, 其中

$$b_0 = a_0^{-1}\ ,\ b_1 = -\frac{b_0 a_1}{a_0}\ ,\ \cdots, b_n = -\frac{a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1}}{a_0}\ ,\ \cdots$$

则 $f(x)g(x) = 1$.

(5) 设 a_0 在 R 中不可约. 若 $f(x)$ 在 $R[[x]]$ 中可约, 则 $f(x) = g(x)h(x)$, 其中

$$g(x) = g_0 + g_1 x + \cdots,\quad h(x) = h_0 + h_1 x + \cdots$$

均非 $R[[x]]$ 中单位. 由 (4) 知 $g_0, h_0 \notin U(R)$. 而 $a_0 = g_0 h_0$, 从而 a_0 在 R 中可约. 矛盾. ■

2.5.13. 设 F 是域, 求证:

(1) 环 $F[[x]]$ 只有一个极大理想 M, 并且 $F[[x]]$ 中全部理想为 M^n $(n = 0, 1, 2, \cdots)$, 其中规定 $M^0 = F[[x]]$. 并且当 $n \neq m$ 时, $M^n \neq M^m$.

(2) $F[[x]]$ 为主理想整环, 从而为 UFD.

证 设 I 是 $F[[x]]$ 的任一非零理想且 $I \neq F[[x]]$, 则 I 不含 $F[[x]]$ 的单位. 由题 2.5.12(4) 知 I 中元的常数项必为 0, 从而 $I \subseteq \langle x \rangle$. 由此可知 $\langle x \rangle$ 是 $F[[x]]$ 的唯一极大理想.

令 $m(x)$ 是非零理想 I 中次数最低的尾 1 的形式幂级数. (注: 形式幂级数

$f(x)=\sum_{n=0}^{\infty}a_nx^n$ 的次数定义为 t, 使得 $a_t\neq 0,\ a_n=0,\ n<t$. 尾 1 是指若 $f(x)$ 的次数为 t, 则 $a_t=1$.) 则 $I=\langle m(x)\rangle$. 事实上, 设 $m(x)=m_0x^t+m_1x^{t+1}+\cdots$, $m_0=1$. 设 $f(x)=a_tx^t+\cdots\in I$. 令 $g(x)=b_0+b_1x+\cdots$, 其中

$$b_0=a_t\ ,b_1=a_{t+1}-b_0m_1,\ \cdots,\ b_n=a_{t+n}-b_{n-1}m_1-\cdots-b_0m_n,\ \cdots,$$

则 $f(x)=m(x)g(x)$. 这就证明了 $F[[x]]$ 是主理想整环.

设 $I=\langle m(x)\rangle$ 是非零理想, $m(x)=x^t+m_1x^{t+1}+\cdots=x^t+g(x)$. 则上述证明说明任一次数 $\geqslant t$ 的形式幂级数可被 $m(x)$ 整除, 从而 $g(x)\in I$. 于是 $x^t\in I$, 这表明 $I=\langle x^t\rangle$, 令 $M=\langle x\rangle$, 则 $F[[x]]$ 的全部理想为

$$0,\ M,\ M^2,\ \cdots,\ M^n=\langle x^n\rangle,\ \cdots.$$

■

2.5.14. $x+1$ 是否为环 $\mathbb{Z}[x]$ 和 $\mathbb{Z}[[x]]$ 中单位? x^2+3x+2 是否为 $\mathbb{Z}[x]$ 和 $\mathbb{Z}[[x]]$ 中不可约元?

证 $x+1\notin U(\mathbb{Z}[x])$.

由题 2.5.12(4) 知 $x+1\in U(\mathbb{Z}[[x]])$.

$x^2+3x+2=(x+2)(x+1)$, 故 x^2+3x+2 在 $\mathbb{Z}[x]$ 中可约.

由题 2.5.12(5) 知 x^2+3x+2 在 $\mathbb{Z}[[x]]$ 中不可约. ■

2.5.15*. 设 $f(x)$ 是 $\mathbb{Q}[x]$ 中奇次不可约多项式, α 和 β 是 $f(x)$ 在 $\mathbb{Q}$ 的某个扩域中两个不同的根. 求证 $\alpha+\beta\notin\mathbb{Q}$.

证 否则, 设 $\alpha+\beta\in\mathbb{Q}$. 令 $g(x)=f\left(x+\dfrac{\alpha+\beta}{2}\right)$, $h(x)=g(x)+g(-x)$, 则 $g(x),\ h(x)\in\mathbb{Q}[x]$, 且 $g(x)$ 也是 $\mathbb{Q}[x]$ 中不可约多项式.

设 $h(x)\neq 0$. 因 $g(x)$ 与 $h(x)$ 有公共根 $\alpha-\dfrac{\alpha+\beta}{2}$, 故最大公因子 $(h(x),\ g(x))$ 是次数 $\geqslant 1$ 的 $\mathbb{Q}[x]$ 中的多项式. 又 $f(x)$ 是奇次的, 故 $\deg h(x)<\deg g(x)$, 从而 $(h(x),\ g(x))$ 的次数小于 $g(x)$ 的次数. 这与 $g(x)$ 在 $\mathbb{Q}[x]$ 中不可约相矛盾!

若 $h(x)=0$, 则 $g(x)=-g(-x)$, 从而 $g(x)$ 不含 x 的偶次幂. 于是 $g(x)$ 有因子 x. 这又与 $g(x)$ 在 $\mathbb{Q}[x]$ 中不可约相矛盾! ■

2.5.16*. 设 k 是域, $f(x_1,x_2)$ 和 $g(x_1,x_2)$ 是 $k[x_1,x_2]$ 中两个互素的多项式. 求证在 k 的任意扩域中 $f(x_1,x_2)=0$ 和 $g(x_1,x_2)=0$ 均只有有限多公共解 (x_1,x_2).

证 以 $\deg_1 f$ 表示 $f(x_1,x_2)$ 对 x_1 的次数. 不妨设 $\deg_1 f=n\geqslant 1$, $\deg_1 g=m\geqslant 1,\ n\geqslant m$. 令 $f(x_1,x_2)=f_0(x_2)x_1^n+\cdots$, $g(x_1,x_2)=g_0(x_2)x_1^m+\cdots$. 设

(a,b) 为 $f(x_1,x_2)=0$, $g(x_1,x_2)=0$ 在 k 的扩域 K 中的解. 令

$$h(x_1,x_2)=g_0(x_2)f(x_1,x_2)-f_0(x_2)g(x_1,x_2)x_1^{n-m},$$

则 $h(a,b)=0$ 且 $\deg_1 h<n=\deg_1 f$. 不妨假设 g_0,g 互素 (否则分别用 $\dfrac{g_0}{(g_0,g)}$ 和 $\dfrac{g}{(g_0,g)}$ 来代替 g_0 和 g). 因 g_0,g 互素, 故 $h(x_1,x_2)$ 与 $g(x_1,x_2)$ 也互素.

首先说明不妨设 $h(x_1,x_2)\neq 0$, 否则 $g_0f=f_0gx_1^{n-m}$. 不妨设 $(f_0,g_0)=1$, 于是 $f_0\mid f$, $g_0\mid g$. 从而在 $k[x_1,x_2]$ 中有 $\dfrac{f}{f_0}=\dfrac{g}{g_0}x_1^{n-m}$, 于是 $\dfrac{g}{g_0}\in k[x_1,x_2]$ 是 f 与 g 的公因子. 但 $(f,g)=1$, 故 $g=g_0$. 于是结论已得证.

现在以 $h(x_1,x_2)$ 代替 $f(x_1,x_2)$ 并重复上述过程, 最后得到非零多项式 $\widetilde{h}(x_1,x_2)$ 使得 $\deg_1\widetilde{h}=0$, $\widetilde{h}(a,b)=0$. 于是 $\widetilde{h}(x_1,x_2)=\widetilde{h}(x_2)\neq 0$, $\widetilde{h}(b)=0$. 从而具有有限多个这样的 b.

同理可知也只有有限多个这样的 a. 从而结论得证. ■

第 3 章　域　论

§1 域的扩张

知识要点:

域论的方法之一是将域 K 看成其子域 F 的扩域; 从而也将 K 看成域 F 上的线性空间, 这个线性空间的维数记为 $[K:F]$. 由此得到域扩张次数的公式 (俗称望远镜公式): 若有域扩张 E/K, K/F, 则 $[E:F]=[E:K][K:F]$.

以下我们多在域扩张 K/F 的框架下研究 K.

首先要弄清素域 (即没有真子域的域, 或等价地, 由单位元生成的域) 的结构. 特征为 0 的素域同构于有理数域 $\mathbb{Q}$; 特征为 p (p 为素数) 的素域同构于剩余类环 $\mathbb{Z}_p$; 任一域包含唯一的素域.

设有域扩张 K/F, 则 K 均可写成添加的形式 $F(S)$, 其中 S 是 K 的某个子集, $F(S)$ 是 K 的包含 S 和 F 的最小子域. $F(S)$ 的构造; 研究 $F(S)$ 在某种意义下可归结为研究 F 的单扩域 $F(u)$.

域 F 上的代数元 u 和 u 在 F 上的极小多项式的定义; 域 F 上的超越元的定义. 单扩域的结构.

有限扩域与代数扩域及其关系.

3.1.1. 设 K/F 为域的扩张, 求证:

(1) 若 $[K:F]$ 是素数, 则 $K=F(u)$, 其中 u 是 K 中任一不属于 F 的元.

(2) 若 $u\in K$ 是 F 上奇次代数元, 则 $F(u)=F(u^2)$.

证 (1) 因 u 是 K 中任一不属于 F 的元, 故 $[F(u):F]>1$. 由望远镜公式 $[K:F]=[K:F(u)][F(u):F]$ 以及假设 $[K:F]$ 是素数, 即知 $[F(u):F]=[K:F]$, 从而 $K=F(u)$.

(2) 因 $F(u^2)$ 是 $F(u)$ 的子域, 故有望远镜公式 $[F(u):F]=[F(u):F(u^2)][F(u^2):F]$. 若 $F(u)\neq F(u^2)$, 则 $[F(u):F(u^2)]=[F(u^2)(u):F(u^2)]=2$. 但由题设 $[F(u):F]$ 是奇数, 矛盾! ■

3.1.2. 求元 a 在域 F 上的极小多项式, 其中

(1) $a=\sqrt{2}+\sqrt{3}$, $F=\mathbb{Q}(\sqrt{6})$;

(2) $a=\sqrt{2}+\sqrt{3}$, $F=\mathbb{Q}(\sqrt{2})$;

(3) $a=\sqrt{2}+\sqrt{3}$, $F=\mathbb{Q}$.

解 (1) 因 a 是二次多项式 $x^2-(5+2\sqrt{6})$ 的根且 $a\notin F$, 故 a 在域 F 上的极小多项式是 $x^2-(5+2\sqrt{6})$.

(2) 同理, a 在域 F 上的极小多项式是 $x^2-2\sqrt{2}x-1$.

(3) 有理数域上以 a 为根的次数最低的首 1 多项式为 x^4-10x^2+1, 即 x^4-10x^2+1 是 a 在域 F 上的极小多项式. ■

3.1.3. 设 u 属于 F 的某个扩域, 并且 u 在 F 上代数. 如果 $f(x)$ 为 u 在 F 上的极小多项式, 则 $f(x)$ 必为 $F[x]$ 中不可约多项式. 反之, 若 $f(x)$ 是 $F[x]$ 中首 1 不可约多项式, 并且 $f(u)=0$, 则 $f(x)$ 为 u 在 F 上的极小多项式.

证 由定义直接证明 (后一结论利用 $F[x]$ 中的带余除法). ■

3.1.4. 设 u 是域 F 的某扩域中的元, 并且 x^n-a 是 u 在 F 上的极小多项式. 对于 $m|n$, 求 u^m 在域 F 上的极小多项式.

解 $x^{\frac{n}{m}}-a$. ■

3.1.5. 设 K/F 为域的代数扩张, D 为整环并且 $F\subseteq D\subseteq K$, 求证 D 为域.

证 $\forall\, 0\neq d\in D$, 则 $d\in K$, d 是 F 上的代数元. 因此 $d^{-1}\in F(d)$, 从而 $d^{-1}\in D$. ■

3.1.6. 设 K/F 为域扩张, $a\in K$. 若 $a\in F(a^m)$, $m>1$, 则 a 在 F 上代数.

证 因 $a\in F(a^m)$, 故存在 $f(x),\ g(x)\in F[x]$ 使得 $a=\dfrac{f(a^m)}{g(a^m)}$. 因此 a 是多项式 $h(x)=xg(x^m)-f(x^m)\in F[x]$ 的根. 设 $f(x)$ 和 $g(x)$ 的次数分别是 s 和 t, 则 $f(x^m)$ 和 $xg(x^m)$ 的次数分别是 ms 和 $mt+1$. 因为 $m>1$, $ms\neq mt+1$, 从而 $h(x)$ 是非零多项式. 于是 a 在 F 上代数. ■

3.1.7. 设 u 是多项式 x^3-6x^2+9x+3 的一个实根.

(1) 求证 $[\mathbb{Q}(u):\mathbb{Q}]=3$;

(2) 将 u^4, $(u+1)^{-1}$, $(u^2-6u+8)^{-1}$ 表示成 1, u, u^2 的 $\mathbb{Q}$– 线性组合.

证 (1) 由 Eisenstein 判别法知 x^3-6x^2+9x+3 在 $\mathbb{Q}$ 上不可约, 即 $[\mathbb{Q}(u):\mathbb{Q}]=3$.

(2) 由题设, 有

$$u^3=6u^2-9u-3,$$
$$u^4=6u^3-9u^2-3u=6(6u^2-9u-3)-9u^2-3u=27u^2-57u-18.$$

设 $(u+1)^{-1}=a+bu+cu^2$, $a,b,c\in\mathbb{Q}$. 则

$$\begin{aligned}1&=(u+1)(a+bu+cu^2)=a+bu+cu^2+au+bu^2+cu^3\\&=a+(a+b)u+(b+c)u^2+c(6u^2-9u-3)\\&=(a-3c)+(a+b-9c)u+(b+7c)u^2.\end{aligned}$$

比较两边 u 的系数, 得到线性方程组

$$\begin{cases} a \quad\; -3c=1, \\ a+b-9c=0, \\ \quad\; b+7c=0. \end{cases}$$

解得 $(u+1)^{-1}=\dfrac{1}{13}(u^2-7u+16)$.

同理, 由待定系数法可算出 $(u^2-6u+8)^{-1}=\dfrac{1}{35}(u^2-9u+1)$. ■

3.1.8. 设 p 为素数, 求扩张 $\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}})/\mathbb{Q}$ 和 $\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{8}})/\mathbb{Q}$ 的次数.

解 $\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}}$ 满足 $x^{p-1}+x^{p-2}+\cdots+x+1=0$. 而 $x^{p-1}+x^{p-2}+\cdots+x+1=0$ 是 $\mathbb{Q}[x]$ 中不可约多项式, 故 $[\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}}):\mathbb{Q}]=p-1$.

因 $\mathrm{e}^{\frac{2\pi\mathrm{i}}{8}}$ 是 $\mathbb{Q}[x]$ 中不可约多项式 $x^4+1=0$ 的根, 故 $[\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{8}}):\mathbb{Q}]=4$. ■

3.1.9. 设 x 是 $\mathbb{Q}$ 上的超越元, $u=x^3/(x+1)$. 求 $[\mathbb{Q}(x):\mathbb{Q}(u)]$.

解 可以验证 x 在 $\mathbb{Q}(u)$ 上的极小多项式为 T^3-uT-u. 从而 $[\mathbb{Q}(x):\mathbb{Q}(u)]=[\mathbb{Q}(u)(x):\mathbb{Q}(u)]=3$. ■

3.1.10. (1) 设 K/F 是域的扩张, 求证 $M=\{a\in K \mid a$ 在 F 上代数 $\}$ 为 K 的一个包含 F 的子域 (称作 F 在 K 中的代数闭包).

(2) 设 K/F 为域的扩张, K 是代数封闭域. 则 (1) 中的域 M 是 F 的一个代数闭包 (即 M 是代数封闭域且 M/F 是代数扩张).

证 (1) 设 α, $0\neq\beta\in M$, 则 $\alpha-\beta$, $\alpha\beta^{-1}\in F(\alpha,\beta)$. 而 $F(\alpha,\beta)$ 是 F 的有限扩域, 从而是 F 的代数扩域. 于是 $\alpha-\beta$, $\alpha\beta^{-1}$ 在 F 上代数, 即 $\alpha-\beta,\alpha\beta^{-1}\in M$, 即 M 是 K 的包含 F 的子域.

(2) 首先 M 是代数封闭域: 设 α 是 M 的某一扩域 Ω 中的元且 α 在 M 上代数. 因 M/F 代数, 故 α 在 F 上代数. 可以认为 α 属于 K 的某一扩域 (例如添加 K 的所有代数元于 F 上得到的域). 因 K 是代数封闭域且 α 在 K 上代数, 则 $\alpha\in K$. 从而由定义 $\alpha\in M$.

再由 M 的构造知 M/F 是代数扩张, 即 M 是 F 的一个代数闭包. ■

3.1.11. 设 M/F 为域的扩张, M 中的元 u,v 分别是 F 上的 m 次和 n 次代数元. $K=F(u)$, $E=F(v)$. 求证:

(1) $[KE:F]\leqslant mn$;

(2) 如果 $(m,n)=1$, 则 $[KE:F]=mn$.

证 $[KE:F]=[F(u,v):F]=[F(u)(v):F(u)][F(u):F]=m[F(u)(v):F(u)]=mn'$, 其中 $n'=[F(u)(v):F(u)]$, $n'\leqslant n$.

同理 $[KE:F]=nm'$, 其中 $m'\leqslant m$. 于是 $n\mid[KE:F]$. 因 $(n,m)=1$, 则 $n\mid n'$, 即 $n=n'$. 即此时 $[KE:F]=mn$. ■

3.1.12. 试证: 关于域 K 的以下四个命题是等价的:

(1) K 为代数封闭域;

(2) $K[x]$ 中每个次数 $\geqslant 1$ 的多项式在 $K[x]$ 中均可表示成一些一次多项式的乘积;

(3) $K[x]$ 中每个次数 $\geqslant 1$ 的多项式在 K 中均有根;

(4) $f(x)$ 为 $K[x]$ 中不可约元 $\Longleftrightarrow \deg f(x)=1$.

证 由定义直接推证. ■

3.1.13. 设 $K=\mathbb{Q}(\alpha)$ 为 $\mathbb{Q}$ 的单扩张, 其中 α 在 $\mathbb{Q}$ 上代数. 求证 $|\operatorname{Aut}(K)|\leqslant[K:\mathbb{Q}]$.

证 $\forall\sigma\in\operatorname{Aut}(K)$, 因 $\sigma(1)=1$, 故 $\sigma|_{\mathbb{Q}}=\mathrm{id}$. 从而 $\operatorname{Aut}(K)=\operatorname{Aut}(K/\mathbb{Q})$. 而 σ 只能将 α 送到 β, 其中 $\beta\in\mathbb{Q}(\alpha)$ 仍是 α 在 $\mathbb{Q}$ 上的极小多项式 $f(x)$ 的根. 因此 $|\operatorname{Aut}(K)|=f(x)$ 在 $\mathbb{Q}(\alpha)$ 中相异根的个数 $\leqslant\deg f(x)=[K:\mathbb{Q}]$. ■

3.1.14. 给出域扩张 K/F 的例子, 使得 $K=F(u,v)$, u 和 v 均是 F 上超越元, 但是 $K\ncong F(x_1,x_2)$, 其中 $F(x_1,x_2)$ 表示 F 上两个独立的不定元 x_1, x_2 的有理函数域.

解 取 $F=\mathbb{Q}$, $K=\mathbb{Q}(x,x)=\mathbb{Q}(x)$, x 是 $\mathbb{Q}$ 上的超越元, 但 $K\ncong\mathbb{Q}(x_1,x_2)$. 否则, 设有域同构 $\sigma:\mathbb{Q}(x)\longrightarrow\mathbb{Q}(x_1,x_2)$, $x_1=\sigma(f(x))$, $x_2=\sigma(g(x))$, $f(x)$, $g(x)\in\mathbb{Q}(x)$. 则 $\sigma|_{\mathbb{Q}}=\mathrm{id}$, $x_1=f(u)$, $x_2=g(u)$, $u=\sigma(x)\in\mathbb{Q}(x_1,x_2)$. 令 $u=k(x_1,x_2)$, $g(u)=h(x_1,x_2)=g(k(x_1,x_2))$. 于是 x_2 满足 $\mathbb{Q}(x_1)[T]$ 中的多项式 $T-h(x_1,T)$. 但 x_2 是 $\mathbb{Q}(x_1)$ 上的超越元, 由此推出 $T=h(x_1,T)$. 于是 $x_2=h(x_1,x_2)=g(k(x_1,x_2))$, 从而 $k(x_1,x_2)=ax_2+b$. 从而 $u=ax_2+b$, a, $b\in\mathbb{Q}$. 于是 $x_1=f(u)=f(ax_2+b)$. 矛盾! ■

3.1.15. 如果 u 是 K 上关于文字 $x_1,\cdots,x_n$ 的有理函数 (即 $u\in K(x_1,\cdots,x_n)$), 但是 $u\notin K$, 求证 u 在 K 上超越.

证 若 u 在 K 上代数, 则存在 $m\geqslant 1$ 使得

$$u^m+a_{m-1}u^{m-1}+\cdots+a_1u+a_0=0\ ,\ a_i\in K\ ,\ i=0,1,\cdots,m-1,a_0\neq 0\ .$$

设 $u=\dfrac{f(x_n)}{g(x_n)}$, $f(x)$, $g(x)$ 均为系数在 $K(x_1,\cdots,x_{n-1})$ 中的多项式, 其中 $(f(x),g(x))=1$. 因 $u\notin K$, 不妨设 $\deg f(x)$ 与 $\deg g(x)$ 不同时为零. 于是

$$a_0g^m(x_n)+a_1g^{m-1}(x_n)f(x_n)+\cdots+f^m(x_n)=0.$$

这样 $f(x_n) \mid g(x_n)$, $g(x_n) \mid f(x_n)$. 于是 $(f(x),g(x)) = f(x)$, $(f(x),g(x)) = g(x)$, 从而 $\deg f(x)$ 与 $\deg g(x)$ 同时为零. 矛盾. ∎

3.1.16. 设 K 是域, x 是 K 上的超越元, $u \in K(x)$, $u \notin K$. 求证 x 在域 $K(u)$ 上代数.

证　设 $u = \dfrac{f(x)}{g(x)}$, $f(x)$, $g(x) \in K[x]$. 于是 x 是 $K(u)[T]$ 中非零多项式 $h(T) := ug(T) - f(T)$ 的根 (因 $u \notin K$, 故比较 $ug(T)$ 和 $f(T)$ 关于 T 的最高次幂的系数就可看出 $h(T) \neq 0$), 即 x 在 $K(u)$ 上代数. ∎

3.1.17. 设 E/F 是域的扩张, 如果对每个元 $\alpha \in E$, $\alpha \notin F$, α 在 F 上均是超越元, 则称 E/F 为纯超越扩张. 求证:

(1) $F(x)/F$ 是纯超越扩张.

(2) 对于任意域扩张 E/F, 求证存在唯一的中间域 M, 使得 E/M 为纯超越扩张, 而 M/F 为代数扩张.

证　(1) 设 $\dfrac{f(x)}{g(x)} \in F(x)$, $\dfrac{f(x)}{g(x)} \notin F$. 若 $\dfrac{f(x)}{g(x)}$ 在 F 上代数, 则由定义容易推出 x 在 F 上代数, 矛盾. 因此 $F(x)/F$ 是纯代数超越扩张.

(2) 令 $M = \{m \in E \mid m \text{ 在 } F \text{ 上代数}\}$, 则 M 是 E 的子域, $M \supseteq F$ 且 M/F 是代数扩张. 下证 E/M 是纯超越扩张. 设 $\alpha \in E$, $\alpha \notin M$. 若 α 是 M 上的代数元, 则由已知定理知 α 也是 F 上的代数元, 从而由 M 的定义 $\alpha \in M$. 矛盾. ∎

§2　分　裂　域

知识要点:

域 F 上多项式 $f(x)$ 在 F 上的分裂域的定义、存在性与意义 (从此, 可保证 $f(x)$ 在 F 的扩域中"全部"根的存在性. 而研究 F 上多项式的根的状况是研究 F 的基本内容和方法).

域 F 上多项式 $f(x)$ 有重根当且仅当 $(f(x), f'(x)) \neq 1$, 其中 $f'(x)$ 是 $f(x)$ 的形式导数. 若 $f(x)$ 在 F 上不可约, 则 $(f(x), f'(x)) \neq 1$ 当且仅当 $f'(x) = 0$ (这只能在 $\operatorname{char} F = p > 0$ 时发生), 当且仅当存在 $g(x) \in F[x]$ 使得 $f(x) = g(x^p)$.

域 F 上正次数多项式 $f(x)$ 称为 F 上的可分多项式, 如果 $f(x)$ 在 $F[x]$ 中的不可约因子均无重根.

同构延拓定理: 设 $\sigma : F \longrightarrow F'$ 是域同构, $f(x)$ 是 $F[x]$ 中的正次数多项式, E 和 E' 分别是 $f(x)$ 在 F 上和 $f^\sigma(x)$ 在 F' 上的分裂域. 则 σ 可延拓成域同构 $E \longrightarrow E'$; 这种延拓的个数 m 满足 $1 \leqslant m \leqslant [E:F]$; 进而, 若 $f(x)$ 是 F 上的可分多项式, 则 $m = [E:F]$ (**注:** 事实上, $m = [E:F]$ 当且仅当 $f(x)$ 是 F 上的可分多项式. 参见题 3.6.7).

同构延拓定理是一条基本定理, 具有重要的应用: 例如, 由此可推出分裂域的唯一性; 亦可得到域 F 上多项式 $f(x)$ 在 F 上的分裂域 E 的 Galois 群 $\mathrm{Gal}(E/F)$ 的阶的估计: $|\mathrm{Gal}(E/F)| \leqslant [E:F]$; 进而, 若 $f(x)$ 是 F 上的可分多项式, 则取等号 (事实上,

$$|\mathrm{Gal}(E/F)| = [E:F]$$

当且仅当 $f(x)$ 是 F 上的可分多项式. 参见上注).

n 次本原单位根.

3.2.1. 写出二元域 $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ 上一个二次不可约多项式 $f(x)$. 将 $f(x)$ 的一个根添加到 $\mathbb{Z}_2$ 中, 写出域 $\mathbb{Z}_2(u)$ 的全部元以及它们的加法表和乘法表.

解 $\mathbb{Z}_2$ 上唯一的二次不可约多项式为 $f(x) = x^2 + x + 1$.$\mathbb{Z}_2(u) = \{0, 1, u, u+1\}$. $\mathbb{Z}_2(u)$ 的全部元的加法表和乘法表如下:

+	0	1	u	u+1
0	0	1	u	u+1
1	1	0	u+1	u
u	u	u+1	0	1
u+1	u+1	u	1	0

·	1	u	u+1
1	1	u	u+1
u	u	u+1	1
u+1	u+1	1	u

■

3.2.2. 设 $f(x)$ 是 $K[x]$ 中多项式, $\deg f(x) = n \geqslant 1$. 求证存在 K 的某个扩域 E, 使得 $[E:K] \leqslant n!$, 并且 $f(x)$ 在 $E(x)$ 中分解成 n 个一次多项式之积.

证 $f(x)$ 在 K 上的分裂域 E 有此性质. ■

3.2.3*. (1) 设 n 是正整数, 域 F 的特征为零或与 n 互素. 则多项式 $x^n - 1 \in F[x]$ 在 K 中的根集 G 是 n 阶循环群, 其中 K 是 $x^n - 1$ 在 F 上的分裂域的任一扩域.

G 的生成元称为 n 次本原单位根. 换言之, 当 F 的特征为零或与 n 互素, F 的某一扩域含有 n 次本原单位根.

(2) 域的乘法群的任一有限子群均是循环群.

证 (1) 因为 F 的特征为零或与 n 互素, 故多项式 $x^n - 1 \in F[x]$ 无重根. 从而 G 是 K^* 的 n 阶子群. 设 $n = p_1^{r_1} \cdots p_m^{r_m}$, $p_1, \cdots, p_m$ 是互不相同的素数, $r_i \geqslant 1, 1 \leqslant i \leqslant m$. 因 n 与 F 的特征互素, 故方程 $x^{\frac{n}{p_i}} - 1 = 0$ 在 K 中恰有 $\dfrac{n}{p_i}$ 个两两不同的解, 故在 G 中存在 a_i 使得 $a_i^{\frac{n}{p_i}} \neq 1$. 令 $b_i = a_i^{n/(p_i^{r_i})}$, 则 $b_i^{p_i^{r_i}} = a_i^n = 1$. 而 $b_i^{p_i^{r_i - 1}} = a_i^{\frac{n}{p_i}} \neq 1$, 因此 b_i 的阶为 $p_i^{r_i}$, 于是 $b_1 \cdots b_m \in G$ 的阶为 n, 故 G 是 n 阶循环群.

(2) 设 G 是域 F 的乘法群 F^* 的任一 n $(n<\infty)$ 阶子群. 则 $a^n=1$, $a\in G$, 故 G 中元均是 $x^n-1\in F[x]$ 的根. 从而 n 与域 F 的特征互素 (否则 x^n-1 在 F 中有重根, 从而在 F 中的不同根的个数小于 n. 矛盾!). 于是 G 恰是 $x^n-1\in F[x]$ 的根集. 由 (1) 知 G 是循环群. ■

3.2.4. 设 F 是特征不为 2 的域, 求证 F 的每个二次扩张均有形式 $F(\sqrt{d})$, $d\in F$. 如果 $\operatorname{char} F=2$, 结论是否成立?

证 设 E/F 是二次扩张, 则 $E=F(r)$, $r\notin F$. 设 r 在 F 上的极小多项式为 $f(r)=x^2+ax+b$, 则 $r+\dfrac{a}{2}$ 在 F 上的极小多项式为 $x^2+\dfrac{b-4a^2}{4}$. 令 $d=\dfrac{4a^2-b}{4}$, 则 $E=F(r)=F\left(r+\dfrac{a}{2}\right)$, 其中 $\left(r+\dfrac{a}{2}\right)^2=d$. 因此 $E=F(r)=F(\sqrt{d})$.

若 $\operatorname{char} F=2$, 则上述结论不成立. 例如, 设 u 是 $x^2+x+1\in\mathbb{Z}_2[x]$ 在其分裂域中的一个根, 则 $\mathbb{Z}_2(u)$ 是 $\mathbb{Z}_2$ 的二次扩张, 但 $\mathbb{Z}_2(u)$ 不能写成 $\mathbb{Z}_2(\sqrt{d})$, $d\in\mathbb{Z}_2$ 的形式. 事实上 $\mathbb{Z}_2(\sqrt{d})=\mathbb{Z}_2$, $\forall\ d\in\mathbb{Z}_2$. ■

3.2.5. 设 F 为域, $c\in F$, p 为素数. 求证: x^p-c 在 $F[x]$ 中不可约 $\Longleftrightarrow$ x^p-c 在 F 中无根.

证 $\Longrightarrow$: 若 x^p-c 在 F 中有根 u, 则在 $F[x]$ 中有 $x^p-c=x^p-u^p=(x-u)^p$, 即 x^p-c 在 $F[x]$ 中可约.

$\Longleftarrow$: 令 u 是 x^p-c 在 F 的某一扩域 E 中的一个根, 则在 $E[x]$ 中 $x^p-c=(x-u)^p$. 若 x^p-c 在 $F[x]$ 中可约, 则 $(x-u)^t$ 是 $F[x]$ 中的多项式, 其中 $1\leqslant t<p$. 于是 $tu\in F$, $0\neq t\in F$. 故 $u\in F$, 即 x^p-c 在 F 中有根. ■

3.2.6*. 设 F 是特征 p 域, p 为素数, $c\in F$.

(1) 求证: x^p-x-c 在 $F[x]$ 中不可约 $\Longleftrightarrow$ x^p-x-c 在 F 中无根.

(2) 如果 $\operatorname{char}F=0$, 试问 (1) 中结论是否仍旧成立?

证 (1) $\Longrightarrow$: 若 x^p-x-c 在 F 中有根 α, 则在 $F[x]$ 中

$$x^p-x-c=(x-\alpha)\frac{x^p-x-c}{x-\alpha},\ 其中\ \frac{x^p-x-c}{x-\alpha}\in F[x].$$

这与 x^p-x-c 在 $F[x]$ 中不可约相矛盾.

$\Longleftarrow$: 设 u 是 x^p-x-c 在 F 的某一扩域 E 中的一个根, 则 $u,u+1,\cdots,u+p-1$ 是其全部根. 因此, 若 x^p-x-c 在 $F[x]$ 中可约, 则 $x-u,x-(u+1),\cdots,x-(u+p-1)$ 中有 t 个一次多项式之积在 $F[x]$ 中, 其中 $1\leqslant t<p$. 这 t 个一次多项式之积的次高项系数在 F 中, 从而 $tu\in F$. 但 $t\neq 0$, 故 $u\in F$, 即 x^p-x-c 在 F 中有根 u.

(2) 如果 $\operatorname{char}F=0$, (1) 中结论一般不再成立. 例如, $x^5-x+15=(x^2+x+3)(x^3-x^2-2x+5)\in\mathbb{Q}[x]$. ■

3.2.7*. 设 F 为域, E 是 $F[x]$ 中 n 次多项式 $f(x)$ 在 F 上的分裂域. 求证 $[E:F] \mid n!$.

证　对 n 用数学归纳法. 分两种情况考虑.

若 $f(x)$ 是 $F[x]$ 中不可约多项式, x_1 是 $f(x)$ 的一个根, 则

$$[E:F] = [E:F(x_1)][F(x_1):F] = n[E:F(x_1)].$$

而 E 恰是 $\dfrac{f(x)}{x-x_1}$ 在 $F(x_1)$ 上的分裂域, 因此由归纳假设知 $[E:F(x_1)] \mid (n-1)!$. 于是 $[E:F] \mid n!$.

若 $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$, 且 $g(x)$ 的次数 m 和 $h(x)$ 的次数均不小于 1. 令 K 为 $g(x)$ 在 F 上的分裂域, 则 E 为 $h(x)$ 在 K 上的分裂域. 因此由归纳假设知 $[E:F] = [E:K][K:F] \mid (n-m)!m! \mid n!$. ■

3.2.8.　设 E 为 x^8-1 在 $\mathbb{Q}$ 上的分裂域. 求 $[E:\mathbb{Q}]$, 并决定 Galois 群 $\mathrm{Gal}(E/\mathbb{Q})$.

解　因为

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1),$$

故 $E = \mathbb{Q}(\mathrm{i}, \sqrt{2})$, 从而 $[E:\mathbb{Q}] = 4$. 因 $x^8-1 \in \mathbb{Q}[x]$ 无重根, 故 $|\mathrm{Gal}(E/F)| = 4$ 且 $\mathrm{Gal}(E/F) = \{\sigma_0 = \mathrm{id}, \sigma_1, \sigma_2, \sigma_3\} = K_4$ (Klein 四元群), 其中 $\sigma_1 : \sqrt{2} \longmapsto -\sqrt{2}$, $\mathrm{i} \longmapsto \mathrm{i}$; $\sigma_2 : \sqrt{2} \longmapsto \sqrt{2}$, $\mathrm{i} \longmapsto -\mathrm{i}$; $\sigma_3 : \sqrt{2} \longmapsto -\sqrt{2}$, $\mathrm{i} \longmapsto -\mathrm{i}$. ■

§3　有限域的结构

知识要点:

由于有限域在理论和应用上的重要性, 我们分三节详细讨论.

有限域的结构定理: 有限域 F 的特征为素数 p; 它是素域 $\mathbb{Z}_p$ 上的 n $(n < \infty)$ 维线性空间, 从而 $|F| = p^n$; F 的加法群是 n 个 p 阶循环群的直和; 其乘法群是 p^n-1 阶循环群, 从而 F 是 $\mathbb{Z}_p$ 的单扩域 $\mathbb{Z}_p(u)$, 其中 u 是 $\mathbb{Z}_p$ 上的 n 次代数元;F 恰是多项式 $x^{p^n} - x \in \mathbb{Z}_p[x]$ 的 p^n 个根作成的集合, 又恰为 $x^{p^n} - x \in \mathbb{Z}_p[x]$ 在 $\mathbb{Z}_p$ 上的分裂域; 从而 p^n 元域总存在, 且在同构意义下唯一. p^n 元域 F 的自同构群恰为 Galois 群 $\mathrm{Gal}(F/\mathbb{Z}_p)$: 它是由 Frobenius 自同构 $a \mapsto a^p$ 生成的 n 阶循环群.

有限域的具体构造: 构造一个 p^n 元域, 只要而且必须找到 $\mathbb{Z}_p$ 上的一个 n 次 (首 1) 不可约多项式 $f(x)$; 然后取其一个根 u, 就得到 (唯一的) p^n 元域 $F = \mathbb{Z}_p(u)$ (于是, F 的加法和乘法结构便自然地确定. 例如, 其乘法由 $f(u) = 0$ 决定).

有限域的子域: p^n 元域的全部子域为 p^m 元域, 其中 m 取遍 n 的正因子. 特别地, p^n 元域只有唯一的 p^m 元子域: 这里的唯一性是指集合意义下的.

Wedderburn 定理: 有限体是域.

以下用 F_q 表示 q 元域, 用 F_q^* 表示 F_q 的乘法群 $F_q-\{0\}$, 其中 q 为素数 p 的幂. 特别地, $F_p=\mathbb{Z}_p$.

3.3.1. (1) 列出 $\mathbb{Z}_2$ 上全部次数小于 5 的不可约多项式.

(2) 列出 $\mathbb{Z}_3$ 上全部二次不可约多项式.

解 (1) $\mathbb{Z}_2[x]$ 中次数小于 5 的不可约多项式为 x, $x+1$, x^2+x+1, x^3+x+1, x^3+x^2+1, $x^4+x^3+x^2+x+1$, x^4+x+1, x^4+x^3+1.

(2) $\mathbb{Z}_3[x]$ 中二次不可约多项式为 x^2+1, x^2+x+2, x^2+2x+2, $2x^2+2$, $2x^2+2x+1$, $2x^2+x+1$. ■

3.3.2. 构作一个 8 元域, 并指出它的加法法则和乘法法则.

解 令 u 是 $\mathbb{Z}_2[x]$ 中三次不可约多项式 x^3+x+1 的一个根, 则 $\mathbb{Z}_2(u)$ 是 8 元域:

$$\begin{aligned}\mathbb{Z}_2(u)&=\{a+bu+cu^2 \mid a,b,c\in\mathbb{Z}_2\}\\&=\{0,\ 1=u^7,\ u,\ u+1=u^3,\ u^2,\\&\quad u^2+1=u^6,\ u^2+u=u^4,\ u^2+u+1=u^5\},\end{aligned}$$

这个表达给出了 $\mathbb{Z}_2(u)$ 的乘法法则, 它由 $u^3=u+1$ 确定; 其加法按 $(a_1+b_1u+c_1u^2)+(a_2+b_2u+c_2u^2)=(a_1+a_2)+(b_1+b_2)u+(c_1+c_2)u^2$ 运算, 其中 $a_i,\ b_i,\ c_i\in\mathbb{Z}_2, i=1,2$. ■

3.3.3. 给出 9 元域 $\mathbb{Z}_3(u)$ 和 9 元域 $\mathbb{Z}_3(v)$ 之间的一个同构, 其中 u 和 v 分别是 $\mathbb{Z}_3[x]$ 中多项式 x^2+1 和 x^2+x+2 的根.

解 因

$$(v+2)^2+1=v^2+v+2=0,$$

故 $v+2$ 在 $\mathbb{Z}_3$ 上的极小多项式也是 x^2+1. 从而有域同构

$$f:\ \mathbb{Z}_3(u)\longrightarrow\mathbb{Z}_3(v+2)=\mathbb{Z}_3(v),$$

其中 $f(a)=a,\ \forall\ a\in\mathbb{Z}_3,\ f(u)=v+2$.

注意: 因 u 和 v 在 $\mathbb{Z}_3$ 上的极小多项式不同, 所以不存在域同构 $g:\mathbb{Z}_3(u)\longrightarrow\mathbb{Z}_3(v)$ 使得 $g(u)=v$. ■

3.3.4. (1) p^n 元域 $F=\mathbb{Z}_p(u)$ 中的 u 是否一定是乘法循环群 F^* 的生成元?

(2) 若 n 和 2^n-1 均是素数, 2^n 元域 $\mathbb{Z}_2(u)$ 中的元 u 是否一定是其乘法循环群的生成元?

解 (1) 未必. 例如, 令 u 是 $x^2+1\in\mathbb{Z}_3[x]$ 的一个根, 则 $u^4=(u^2)^2=(-1)^2=1$. 故 u 不是 9 元域 $\mathbb{Z}_3(u)$ 乘法群的生成元.

(2) 一定是: 因为此时乘法群 $(\mathbb{Z}_2(u))^*$ 是素数阶循环群, 故其任一非单位元的元均是生成元. 因 $u\neq 1$, 从而 u 是生成元. ■

3.3.5. $F_q[x]$ 中 n 次首 1 不可约多项式 $f(x)$ 称为 $F_q[x]$ 中的 n 次本原多项式 (注意: 这里的本原和 2.5 节中本原的意义完全不同), 如果 $f(x)$ 的某一根 u 是域 $F_q(u)$ 的乘法循环群的生成元.

(1) 证明 x^4+x+1 为 $\mathbb{Z}_2[x]$ 中本原多项式.

(2) 列出 16 元域 $\mathbb{Z}_2(u)$ 中 (唯一的) 4 元子域 F_4 的全部元, 这里 u 是 $x^4+x+1\in\mathbb{Z}_2[x]$ 的一个根.

(3) 求出 u 在 4 元域上的极小多项式.

证 (1) 设 u 是 x^4+x+1 的一个根. 显然 $u,\ u^2,\ u^3$ 均不是 1, $u^4=u+1\neq 1$, $u^5=u^2+u\neq 1$, $u^6=u^3+u^2\neq 1$, $u^7=u^3+u+1\neq 1$, $u^8=u^2+1\neq 1$, $u^9=u^3+u\neq 1$, $u^{10}=u^2+u+1\neq 1$, $u^{11}=u^3+u^2+u\neq 1$, $u^{12}=u^3+u^2+u+1\neq 1$, $u^{13}=u^3+u^2+1\neq 1$, $u^{14}=u^3+1\neq 1$, $u^{15}=1$. 因此, u 是 $\mathbb{Z}_2(u)$ 的乘法群的生成元.

(2) $F_4=\{0,\ 1,\ u^5,\ u^{10}\}$.

(3) $x^2+x+u^5\in F_4[x]$. ■

3.3.6. (1) 证明 $x^4+x^3+x^2+x+1$ 为 $\mathbb{Z}_2[x]$ 中不可约多项式但不是本原多项式.

(2) 令 u 为 $x^4+x^3+x^2+x+1\in\mathbb{Z}_2[x]$ 的一个根, 试问 $F_{16}=\mathbb{Z}_2(u)$ 中哪些元是 F_{16} 的乘法群的生成元?

证 (1) 设 $u^4+u^3+u^2+u+1=0$, 则 $u^5=1$. 因此 $u^4+u^3+u^2+u+1$ 不是本原多项式.

(2) F_{16} 的乘法生成元有 $\varphi(15)=8$ 个, 它们是

$$u+1,\ u^2+u,\ u^2+1,\ u^2+u+1,\ u^3+1,\ u^3+u,\ u^3+u+1,\ u^3+u^2+u.$$ ■

3.3.7. 设 F 为 q 元域, $q=p^n$, p 为素数, H 是 $\mathrm{Aut}(F)$ 的 m 阶子群, $K=\{a\in F\mid$ 对每个 $\alpha\in H,\ \alpha(a)=a\}$. 求证:

(1) $m|n$;

(2) K 是 F 中唯一的 $p^{n/m}$ 元子域.

证 (1) 因 $\mathrm{Aut}(F)$ 是 n 阶群, H 是 $\mathrm{Aut}(F)$ 的 m 阶子群, 故由 Lagrange 定理知 $m \mid n$.

(2) 因 $\mathrm{Aut}(F) = \langle\sigma\rangle$ 是 n 阶循环群, 其中 $\sigma(a) = a^p, \forall a \in F$, 故 $\mathrm{Aut}(F)$ 的 m 阶子群只有一个, 即 $H = \langle\sigma^{\frac{n}{m}}\rangle$. 因此由 K 的定义知

$$K = \{a \in F \mid a^{p^{\frac{n}{m}}} = a\}\ .$$

因此 K 是 F 的 $p^{\frac{n}{m}}$ 元子域, 从而是 F 的唯一 $p^{\frac{n}{m}}$ 元子域. ■

3.3.8. 求证:

(1) $F_{p^n} \supseteq F_{p^m} \Longleftrightarrow m \mid n$.

(2) 设 $F_{p^n} \supseteq F_{p^m}$, 令 $G = \{\sigma \in \mathrm{Aut}(F_{p^n}) \mid$ 对每个 $a \in F_{p^m}, \sigma(a) = a\}$, 则 G 是 n/m 阶循环群.

证 (1) 若 $m \mid n$, 则 $x^{p^m} - x$ 的根均为 $x^{p^n} - x$ 的根, 从而 $F_{p^m} \subseteq F_{p^n}$. 反之, $F_{p^m}^*$ 是 $F_{p^n}^*$ 的子群, 因此 $(p^m - 1) \mid (p^n - 1)$. 令 $n = lm + r$, $0 \leqslant r < m$, 则 $p^n - 1 = p^{lm}p^r - p^r + p^r - 1 = p^r(p^{lm} - 1) + p^r - 1$. 于是 $(p^m - 1) \mid (p^r - 1)$. 这迫使 $r = 0$, 即 $m \mid n$.

(2) 首先易证 G 是 $\mathrm{Aut}(F_{p^n})$ 的子群. 而 $\mathrm{Aut}(F_{p^n}) = \langle\sigma\rangle$ 是 n 阶循环群, 其中 $\sigma(a) = a^p$, $\forall a \in F_{p^n}$. 我们断言 $G = \langle\sigma^m\rangle$, 从而 G 为 $\dfrac{n}{m}$ 阶循环群.

事实上, F_{p^m} 恰是 $x^{p^m} - x$ 的 p^m 个根, 故 $\langle\sigma^m\rangle \leqslant G$. 若 $G \neq \langle\sigma^m\rangle$, 则 $G = \langle\sigma^t\rangle$, $t \mid m, t \neq m$. 则 $a^{p^t} = a, \forall a \in F_{p^m}$, 从而 $F_{p^m} \subseteq F_{p^t}$. 这与 $t < m$ 矛盾. ■

3.3.9. 求证: 代数封闭域必是无限域.

证 否则, 设 F 是 p^n 元代数封闭域, 则 F 是多项式 $x^{p^n} - x$ 的 p^n 个根的集合. 另一方面, 设 E 是 F 上多项式 $x^{p^m} - x$ 在 F 上的分裂域, 其中 $m > n$. 令 ω 是 $p^m - 1$ 次本原单位根, 则 $\omega \in E$ 是 F 上的代数元. 从而由代数封闭域的定义知 $\omega \in F$, 于是 $\omega^{p^n - 1} = 1$. 这与 ω 是 $p^m - 1$ 次本原单位根不合. ■

3.3.10*. 求证: 域 F 是有限域当且仅当 F 的乘法群 F^* 是循环群.

证 熟知有限域的乘法群是循环群. 反之, 设 $F^* = \langle u\rangle$ 是循环群, 则 F^* 必是有限循环群, 从而 F 是有限域. 否则, F^* 中任一元 a $(a \neq 1)$ 的乘法阶必为无限. 但 $(-1)^2 = 1$, 故 F 的特征为 2. 因 $u + 1 \neq 0$, 故 $u + 1 \in F^* = \langle u\rangle$, 于是 $u + 1 = u^n$, 即 u 是 F 的素域 $\mathbb{Z}_2$ 上的代数元. 从而 $F = \mathbb{Z}_2(u)$ 是有限域. 矛盾!

■

3.3.11*. 设 $a, b \in F_{2^n}$, n 是奇数. 若 $a^2+b^2+ab=0$, 则 $a=b=0$.

证 设 $F_{2^n}=\mathbb{Z}_2(u)$, 其中 u 是循环群 $F_{2^n}^*$ 的生成元. 设 $a^2+b^2+ab=0$, 并假设 a,b 之一不为零, 则由题设 $a\neq 0\neq b$, 且 $a\neq b$. 从而 $a=u^i$, $b=u^j$, $i\neq j$, $1\leqslant i,j\leqslant 2^n-1$. 由 $a^2+b^2+ab=0$ 即可推出存在 t 使得 $u^{2t}+u^t+1=0$, 其中 $1\leqslant t<2^n-1$. 这表明 u^t 在 $\mathbb{Z}_2$ 上的极小多项式为 x^2+x+1 (这是因为 $u^t\neq 1$). 于是

$$n=[\mathbb{Z}_2(u):\mathbb{Z}_2]=[\mathbb{Z}_2(u):\mathbb{Z}_2(u^t)][\mathbb{Z}_2(u^t):\mathbb{Z}_2]=2[\mathbb{Z}_2(u):\mathbb{Z}_2(u^t)].$$

这与 n 是奇数相矛盾! ■

3.3.12*. 设 F 是有限域, $a,b\in F^*$. 求证: 对每个 $c\in F$, 方程 $ax^2+by^2=c$ 在域 F 中均有解 (x,y).

特别地, 有限域的任意元均可写成两个元的平方和.

证 即要证对任一 $a\in F^*$ 和 $b\in F$, 方程 $x^2+ay^2=b$ 在 F 中均有解 (x,y).

设 $\operatorname{char}F=2$, $F^*=\langle u\rangle$, 且不妨设 $b=u^i$. 若 i 是偶数, 方程 $x^2+ay^2=b$ 在 F 中有解 $(u^{\frac{i}{2}},0)$. 若 i 是奇数, 方程 $x^2+ay^2=b$ 在 F 中有解 $(u^{\frac{i+|F|-1}{2}},0)$.

下设 $\operatorname{char}F=p\neq 2$. 若结论不成立, 即存在 $a\in F^*$ 和 $b\in F$ 使得 $x^2=b-ay^2$ 在 F 中无解. 令 $\Omega_1=\{x^2\mid x\in F\}$, $\Omega_2=\{b-ay^2\mid y\in F\}$.

首先计算 $|\Omega_1|$. 设 $F=\{0,u,u^2,\cdots,u^{|F|-1}\}$. 注意到 $|F|-1$ 是偶数, 故 $\Omega_1=\left\{0,u^{2i}\mid 1\leqslant i\leqslant \dfrac{|F|-1}{2}\right\}$. 由此知

$$|\Omega_1|=\frac{|F|-1}{2}+1.$$

又因为 $x^2\mapsto b-ax^2$ 给出了 Ω_1 到 Ω_2 的一个一一映射, 因此

$$|\Omega_2|=|\Omega_1|=\frac{|F|-1}{2}+1.$$

而 $x^2=b-ay^2$ 在 F 中无解说明 $\Omega_1\bigcap\Omega_2=\varnothing$. 从而 $|F|\geqslant 2\left(\dfrac{|F|-1}{2}+1\right)=|F|+1$. 矛盾. ■

3.3.13*. 设 $F=F_q$, $(n,q)=1$, E 为 x^n-1 在 F 上的分裂域. 求证: $[E:F]$ 是满足 $n|(q^k-1)$ 的最小正整数 k.

证 设 $[E:F]=k$, 则 $|E|=|F|^k=q^k$, $|E^*|=q^k-1$. 因 $(n,q)=1$, 故 x^n-1 无重根, 从而 x^n-1 的 n 个根作成 n 阶循环群. 设 ω 是这个循环群的一个生成元, 则 $E=F(\omega)$, $\omega\in E^*$, 从而 $n|(q^k-1)$.

设 $n|(q^s-1)$, 则 $\omega^{q^s-1}=1$, 从而 $\omega\in F_{q^s}$. 又 $F=F_q\subseteq F_{q^s}$, 故 $E\subseteq F_{q^s}$. 于是 $k=[E:F]\leqslant[F_{q^s}:F]=s$, 即 $[E:F]$ 是满足 $n|(q^k-1)$ 的最小正整数. ■

3.3.14*. 设 $c\in F_q^*$, m 为正整数. 则

(1) 方程 $x^m=c$ 在 F_q 中有解当且仅当 $c^{\frac{q-1}{(q-1,m)}}=1$.

(2) 若 $x^m=c$ 在 F_q 中有解, 它恰有 $(q-1,m)$ 个解.

(3) F_q^* 中恰有 $\dfrac{q-1}{(q-1,m)}$ 个元 c, 使得方程 $x^m=c$ 在 F_q 中有解.

(4) F_q 中任一元均是 F_q 中某一元的 m 次幂当且仅当 $(q-1,m)=1$.

证 (1) 若 $u\in F_q$ 是 $x^m=c$ 的解, 则

$$c^{\frac{q-1}{(q-1,m)}}=(u^m)^{\frac{q-1}{(q-1,m)}}=(u^{\frac{m}{(q-1,m)}})^{(q-1)}=1.$$

反之, 设 $c^{\frac{q-1}{(q-1,m)}}=1$. 因 $\left(\dfrac{q-1}{(q-1,m)},\dfrac{m}{(q-1,m)}\right)=1$, 故存在 $l,t\in\mathbb{Z}$ 使得 $l\dfrac{q-1}{(q-1,m)}+t\dfrac{m}{(q-1,m)}=1$, 从而 $c^{t\frac{m}{(q-1,m)}}=c$. 另一方面, 设 u 是 F_q^* 的生成元, $c=u^s$. 则由 $1=c^{\frac{q-1}{(q-1,m)}}=u^{s\frac{q-1}{(q-1,m)}}$ 可知 $(q-1)\mid s\dfrac{q-1}{(q-1,m)}$. 于是有 $s'\in\mathbb{Z}$ 使得 $s=s'(q-1,m)$. 从而

$$(u^{ts'})^m=(u^{ts'(q-1,m)})^{\frac{m}{(q-1,m)}}=c^{t\frac{m}{(q-1,m)}}=c,$$

即 $u^{ts'}$ 是 $x^m=c$ 的解.

(2) 设 v 是 $x^m=c$ 在 F_q 中的一个解, 则方程 $x^m=c$ 成为 $(v^{-1}x)^m=1$. 故即要求 $x^m=1$ 在 F_q 中解的个解. 存在 $l,t\in\mathbb{Z}$ 使得 $l(q-1)+tm=(q-1,m)$, 因 $a^{q-1}=1$, $\forall\, a\in F_q$, 从而 $x^m=1$ 在 F_q 中解均为方程 $x^{(q-1,m)}=1$ 在 F_q 中解, 反之亦然. 设 $q=p^n$. 故 p 与 $(q-1,m)$ 互素, 从而 $x^{(q-1,m)}=1$ 在 F_q 中解作成 F_q^* 的 $(q-1,m)$ 阶循环子群. 从而 $x^m=c$ 在 F_q 中有 $(q-1,m)$ 个解.

(3) F_q^* 中恰有 $\dfrac{q-1}{(q-1,m)}$ 个元 c, 使得 $c^{\frac{q-1}{(q-1,m)}}=1$. 由 (1) 即知 F_q^* 中恰有 $\dfrac{q-1}{(q-1,m)}$ 个元 c, 使得方程 $x^m=c$ 在 F_q 中有解.

(4) 若 F_q 中任一元均是 F_q 中某一元的 m 次幂, 则由 (3) 知 $\dfrac{q-1}{(q-1,m)}=q-1$, 即 $(q-1,m)=1$; 反之, 若 $(q-1,m)=1$, 则 F_q^* 中任一元 c 满足 $c^{\frac{q-1}{(q-1,m)}}=1$, 故由 (1) 知 F_q^* 中任一元 c 均是 F_q 中某一元的 m 次幂, 即 F_q 中任一元均是 F_q 中某一元的 m 次幂. ■

3.3.15*. 设 q 为素数幂, 求证:

(1) 有限域 F_q 的所有元之和为零, 其中 $q \neq 2$.

(2) 设 $q-1=ds$, d, s 均为正整数且 $s>1$, 则 F_q^* (唯一) 的 s 阶子群的所有元之和为零.

(3) 设 m 为正整数, 则

$$\sum_{a \in F_q} a^m = \begin{cases} -1, & (q-1) \mid m, \\ 0, & (q-1) \nmid m. \end{cases}$$

证 (1) 因 $x^q - x = \prod\limits_{a \in F_q}(x-a)$, 由根与系数的关系知 $-\sum\limits_{a \in F_q} a$ 恰是这个多项式中 x^{q-1} 的系数. 而当 $q \neq 2$ 时, $x^q - x$ 中 x^{q-1} 的系数为零. 由此证得.

(2) 设 u 是 F_q^* 的生成元 (即 u 的乘法阶为 $q-1$), 即要证 $\sum\limits_{0 \leqslant i \leqslant s-1} u^{di} = 0.$

由题设知 $q>2$, 重整和式 $\sum\limits_{a \in F_q} a$:

$$\begin{aligned} 0 = \sum_{a \in F_q^*} a &= 1 + u + u^2 + \cdots + u^{q-2} \\ &= 1 + u + \cdots + u^{d-1} \\ &\quad + u^d(1 + u + \cdots + u^{d-1}) \\ &\quad + u^{2d}(1 + u + \cdots + u^{d-1}) \\ &\quad + \cdots \\ &\quad + u^{(s-1)d}(1 + u + \cdots + u^{d-1}) \\ &= (1 + u^d + u^{2d} + \cdots + u^{(s-1)d})(1 + u + \cdots + u^{d-1}). \end{aligned}$$

因 $1 + u + \cdots + u^{d-1} = \dfrac{u^d - 1}{u-1} \neq 0$, 故 $1 + u^d + u^{2d} + \cdots + u^{(s-1)d} = 0$.

(3) 若 $(q-1) \mid m$, 则

$$\sum_{a \in F_q} a^m = \sum_{a \in F_q^*} a^m = \sum_{a \in F_q} 1 = q-1 = -1.$$

设 $(q-1) \nmid m$. 利用带余除法及 $a^{q-1}=1$, $\forall\, a \in F_q^*$, 不妨设 $m < q-1$. 从而 $d = (q-1, m) < q-1$, $s = \dfrac{q-1}{(q-1,m)} > 1$, $q-1 = ds$.

令 $(F_q^*)^m = \{a^m \mid a \in F_q^*\}$, 则 $(F_q^*)^m$ 是循环群 $F_q^* = \langle u \rangle$ 的子群, 且其阶为 $\dfrac{q-1}{(q-1,m)}$. 故 $(F_q^*)^m = \langle u^d \rangle = \{1, u^d, \cdots, u^{(s-1)d}\}$. 于是由 (2) 知 $\sum\limits_{0 \leqslant i \leqslant s-1} u^{di} = 0.$

另一方面, 考虑群的满同态 $\pi: F_q^* \longrightarrow (F_q^*)^m$, 其中 $\pi(a)=a^m$. 则 $\mathrm{Ker}\ \pi$ 是 F_q^* 的 d 阶子群, $\mathrm{Ker}\ \pi=\langle u^s\rangle=\{1,u^s,\cdots,u^{(d-1)s}\}$, 且有陪集分解

$$F_q^*=\bigcup_{1\leqslant i\leqslant s} u^i\mathrm{Ker}\ \pi.$$

因此

$$\begin{aligned}\sum_{a\in F_q} a^m &= \sum_{a\in F_q^*}\pi(a)=d\sum_{1\leqslant i\leqslant s}\pi(u^i)\\ &=d\sum_{c\in(F_q^*)^m} c=d\sum_{c\in\langle u^d\rangle} c\\ &=d\sum_{0\leqslant i\leqslant s-1} u^{di}=0.\end{aligned}$$

■

§4　有限域上的不可约多项式

知识要点:

有限域 F_{p^n} 的构造归结为 $\mathbb{Z}_p$ 上 n 次不可约多项式的构造. 如何得到 $\mathbb{Z}_p$ 上的 n 次不可约多项式? 一般地, 如何得到 F_q 上的 n 次不可约多项式? 这样的多项式一般当然不止一个, 它们之间有何关系?

有限域上的不可约多项式有深入的理论和算法, 已超出本书的范围. 这里仅涉及其中部分比较基本的问题.

以下用 F_q 表示 q 元域, 其中 q 为素数的幂.

3.4.1. 对每个正整数 n, $F_q[x]$ 中必存在 n 次不可约多项式.

证　总存在 q^n 元域 E: E 是 $x^{q^n}-x\in F_q[x]$ 在 F_q 上的分裂域, 且 $E=F_q(u)$. 于是 u 在 F_q 上的极小多项式就是 $F_q[x]$ 中的 n 次不可约多项式. ■

3.4.2*. 多项式 $x^{q^n}-x$ 是 $F_q[x]$ 中所有次数整除 n 的不可约首 1 多项式的乘积.

特别地, F_q 上任一 n 次不可约首 1 多项式均是 $x^{q^n}-x$ 的次数最高的不可约因子.

证　记 E 为多项式 $x^{q^n}-x$ 在 F_q 上的分裂域, 则 E 恰是 $x^{q^n}-x$ 的 q^n 个根作成的域. 设 $g(x)$ 是 $F_q[x]$ 中的首 1 d 次不可约多项式, 并设 u 是 $g(x)$ 的一个根, 则 $g(x)$ 是 u 在 F_q 上的极小多项式, 从而 $|F_q(u)|=q^d$. 于是

$$g(x)|(x^{q^n}-x)\Longleftrightarrow u^{q^n}-u=0\Longleftrightarrow u\in E\Longleftrightarrow F_q(u)\subseteq E\Longleftrightarrow d\mid n. \qquad (*)$$

将 $f(x):=x^{q^n}-x$ 分解为 $F_q[x]$ 中不可约多项式的乘积. 因 $f(x)$ 首 1, 故不

妨设这些不可约因子均首 1. 因 $f(x)$ 无重根, 故这个分解中每个不可约因子的重数均为 1.

由 $(*)$ 式, $f(x)$ 的每个不可约因子的次数整除 n; 再由 $(*)$ 式, $F_q[x]$ 中任一次数整除 n 的首 1 不可约多项式是 $f(x)$ 的因子, 从而 $F_q[x]$ 中所有 (两两不同) 的次数整除 n 的首 1 不可约多项式的乘积也是 $f(x)$ 的因子. 于是 $f(x)$ 恰是 $F_q[x]$ 中所有次数整除 n 的不可约首 1 多项式的乘积. ■

3.4.3. 设 $f(x)$ 是 $F_q[x]$ 中 n 次首 1 不可约多项式, u 为 $f(x)$ 的一个根. 则

(1) $f(x)$ 共有 n 个彼此不同的根: $u, u^q, \cdots, u^{q^{n-1}}$.

(2) n 是使得 $u^{q^n-1}=1$ 的最小正整数.

(3) 设 l 是 u 的乘法阶, 则 n 是使得 $l \mid q^n-1$ 的最小正整数; 且 $f(x)$ 的任一根的乘法阶均为 l.

证 (1) 因 F_q 中元 a 均满足 $a^q=a$, 从而对任一正整数 t 均有 $a^{q^t}=a$. 于是

$$f(u^{q^t})=(f(u))^{q^t}=0,$$

即 $u, u^q, \cdots, u^{q^{n-1}}$ 均是 $f(x)$ 的根. 而且 $u, u^q, \cdots, u^{q^{n-1}}$ 两两不同: 否则存在 $1\leqslant i<j\leqslant n-1$ 使得 $(u^{q^{j-i}}-u)^{q^i}=u^{q^j}-u^{q^i}=0$, 从而 $u^{q^{j-i}-1}=1$, 于是 $F_q(u)$ 是 q^{j-i} 元域的子域. 但 $F_q(u)$ 是 q^n 元域. 矛盾!

(2) 因 $u\in F_q(u)$ 且 $F_q(u)$ 是 q^n 元域, 故 $u^{q^n-1}=1$. 若 $u^{q^m-1}=1$, m 为正整数, 则 u 属于 $x^{q^m}-x$ 在 F_q 上的分裂域 E, 于是 $F_q(u)\subseteq E$, 从而 $q^n=|F_q(u)|\leqslant|E|=q^m$. 故 $n\leqslant m$.

(3) 由 $u^{q^n-1}=1$ 即知 $l\mid q^n-1$. 若 $l\mid q^m-1$, m 为正整数, 则 $u^{q^m-1}=1$. 与上段同样的证明知 $n\leqslant m$.

最后, $f(x)$ 的任一根形如 u^{q^i}, $1\leqslant i\leqslant n-1$. 因 $(q^i,l)=1$, 故 u^{q^i} 的乘法阶为 $\dfrac{l}{(q^i,l)}=l$. ■

3.4.4. 求证: x^5-x+1 是 $\mathbb{Z}_3[x]$ 中的本原多项式.

证 因 x^5-x+1 无根在 $\mathbb{Z}_3$ 中, 故 x^5-x+1 在 $\mathbb{Z}_3[x]$ 中无一次因子; 又因 $\mathbb{Z}_3[x]$ 中次数为 2 的首 1 不可约多项式为 x^2+1, x^2+x+2, x^2+2x+2; 它们均非 x^5-x+1 的因子. 从而 x^5-x+1 是 $\mathbb{Z}_3[x]$ 中的不可约多项式.

设 u 是 x^5-x+1 的一个根, 即要证 u 的阶 $l=3^5-1$. 因 $l\mid 3^5-1$ (参见题 3.4.3(3)), 且 $l>5$, 故 l 的可能值为 $11, 22, 121, 242$. 由 $u^5=u-1$ 知

$$u^{11}=u(u^5)^2=u(u-1)^2\neq 1;$$

$$u^{22} = (u^{11})^2 = (u(u-1)^2)^2 = u^2(u-1)(u-1)^3 = (u-1)u^2(u^3-1)$$
$$= (u-1)(u^5-u^2) = (u-1)(u-1-u^2) \neq 1;$$

$$u^{121} = u(u^5)^{24} = u(u-1)^{24} = u\frac{(u-1)^{27}}{(u-1)^3} = u\frac{u^{27}-1}{u^3-1},$$

而

$$u^{27} = u^2(u^5)^5 = u^2(u-1)^5 = u^2(u-1)^3(u-1)^2 = u^2(u^3-1)(u-1)^2$$
$$= (u-1-u^2)(u-1)^2 = -(u+1)^2(u-1)^2 = -(u^2-1)^2 = 2u^4+2u^2+2,$$

$$u(u^{27}-1) = 2u^5+2u^3+u = 2(u-1)+2u^3+u = 2(u^3-1).$$

于是 $u^{121} = 2 \neq 1$. 综上所述, u 的阶为 $l = 242$. 这就是所要证明的. ■

3.4.5*. (1) 设 $f(x)$ 是 $F_q[x]$ 中 n 次首 1 不可约多项式. 若 $f(x)$ 的一个根 u 为域 $F_q(u)$ 的乘法循环群 $F_q^*(u)$ 的生成元, 则 $f(x)$ 的每个根也都是 $F_q^*(u)$ 的生成元.

(2) $F_q[x]$ 中 n 次首 1 不可约多项式 $f(x)$ 称为 $F_q[x]$ 中的 n 次本原多项式, 如果 $f(x)$ 的某一根 u 是域 $F_q(u)$ 的乘法循环群的生成元. 证明 $F_q[x]$ 中共有 $\dfrac{\varphi(q^n-1)}{n}$ 个 n 次本原多项式, 其中 $\varphi(n)$ 是 Euler 函数 (即 $\varphi(n)$ 是小于 n 的正整数中与 n 互素的正整数的个数).

证 (1) 若 u 是 $F_q(u)$ 的乘法群的生成元, 则 u 的乘法阶为 q^n-1. 而 $q^t(1 \leqslant t \leqslant n-1)$ 与 q^n-1 互素, 故 $u^q, \cdots, u^{q^{n-1}}$ 均为 q^n-1 阶元, 从而均是循环群 $F_q^*(u)$ 的生成元. 由题 3.4.3(1) 知 $u, u^q, \cdots, u^{q^{n-1}}$ 是 $f(x)$ 的全部的两两不同的根. 故 $f(x)$ 的任一根均是 $F_q^*(u)$ 的生成元.

(2) 设 $F_q[x]$ 中共有 t 个 n 次本原多项式, 它们均为多项式 $x^{q^n}-x$ 的因子. 设 E 是 $x^{q^n}-x$ 的根集作成的 q^n 元域, 则 E 的乘法循环群 E^* 有 $\varphi(q^n-1)$ 个生成元.

由 (1) 知 $F_q[x]$ 中每个 n 次本原多项式的所有根均为 E^* 的生成元. 而 E^* 的任一生成元均是 $F_q[x]$ 中某一 n 次本原多项式的一个根, 从而 E^* 共有 nt 个生成元 (注意到两个不同的 n 次本原多项式互素, 从而没有相同的根). 由此即得. ■

3.4.6*. 求证: 当 $n \geqslant 3$ 时, $x^{2^n}+x+1$ 是 $\mathbb{Z}_2[x]$ 中可约多项式.

证 若 $x^{2^n}+x+1$ 是 $\mathbb{Z}_2[x]$ 中不可约多项式, 则 $|\mathbb{Z}_2(u)| = 2^{2^n}$, 其中 u 是 $x^{2^n}+x+1$ 的一个根. 从而 $u^{2^n} = u+1$, 故

$$u^{2^{2n}} = (u^{2^n})^{2^n} = (u+1)^{2^n} = u^{2^n}+1 = u\ .$$

这表明 u 属于 2^{2n} 元域. 但 2^{2n} 元域中任一元在 $\mathbb{Z}_2$ 上的极小多项式的次数小于或等于 $2n$, 因此

$$2^n \leqslant 2n\ ,\quad 2^{n-1} \leqslant n\ .$$

从而 $n \leqslant 2$. 因此, 当 $n \geqslant 3$ 时, $x^{2^n}+x+1$ 是 $\mathbb{Z}_2[x]$ 中可约多项式. ■

注 称形如 $F_n = 2^{2^n}+1$ 的整数为 Fermat 数. 已知 $F_0, F_1, F_2, F_3 = 257$, $F_4 = 65537$ 均为素数; 但 $F_5 = 641 \times 6700417$.

3.4.7*. Möbius 函数 $\mu:\ \mathbb{N} \longrightarrow \{0,1,-1\}$ 定义如下:

$$\mu(n) = \begin{cases} 1, & \text{若 } n=1, \\ 0, & \text{若 } n \text{ 被素数的平方整除}, \\ (-1)^r, & \text{若 } n \text{ 是 } r \text{ 个互异的素数之积}. \end{cases}$$

则

(1) μ 是积性函数, 即: 若 n 和 m 是互素的正整数, 则 $\mu(mn) = \mu(m)\mu(n)$.

(2) 对于任一正整数 n 有

$$\sum_{d|n} \mu(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) = \begin{cases} 1, & n=1, \\ 0, & n>1. \end{cases}$$

(3) (Möbius 反演律) 设 H 和 h 均为正整数集 $\mathbb{N}$ 到 Abel 群 G 的映射 (G 的运算用加法表示). 若

$$H(n) = \sum_{d|n} h(d),\quad \forall\ n \in \mathbb{N},$$

则

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right),\quad \forall\ n \in \mathbb{N};$$

反之亦然.

证 (1) 根据定义分情况讨论易得.

(2) 不妨设 $n>1$. 设 $p_1, \cdots, p_m$ 是 n 的全部两两不同的素因子, 则

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{1\leqslant i\leqslant m} \mu(p_i) + \sum_{1\leqslant i<j\leqslant m} \mu(p_ip_j) + \cdots + \mu(p_1\cdots p_m) \\ &= 1 + (-1)\binom{m}{1} + (-1)^2\binom{m}{2} + \cdots + (-1)^m\binom{m}{m} \\ &= (1-1)^m = 0. \end{aligned}$$

(3) 设 $H(n)=\sum_{d|n}h(d)$, $\forall\ n\in\mathbb{N}$. 则对于 n 的每个正因子 d 有 $H(d)=\sum_{s|d}h(s)$, 从而

$$\begin{aligned}
\sum_{d|n}\mu\left(\frac{n}{d}\right)H(d) &= \sum_{d|n}\sum_{s|d}\mu\left(\frac{n}{d}\right)h(s)\\
&= \sum_{s|n}\sum_{d,\ s|d|n}\mu\left(\frac{n}{d}\right)h(s)\\
&= \sum_{s|n}h(s)\sum_{d,\ s|d|n}\mu\left(\frac{n}{d}\right)\\
&= \sum_{s|n}h(s)\sum_{t,\ t|\frac{n}{s}}\mu\left(\frac{\frac{n}{s}}{t}\right)\\
&= \sum_{s|n}h(s)\lambda(s),
\end{aligned}$$

其中由本题 (2) 可知

$$\lambda(s)=\sum_{t,\ t|\frac{n}{s}}\mu\left(\frac{\frac{n}{s}}{t}\right)=\begin{cases}1, & 若\ \dfrac{n}{s}=1,\\ 0, & 若\ \dfrac{n}{s}\neq 1.\end{cases}$$

从而

$$\sum_{d|n}\mu\left(\frac{n}{d}\right)H(d)=h(n).$$

反之, 同理可证. ■

3.4.8*. 求证: 有限域 F_q 上 n 次首 1 不可约多项式的个数 $N_q(n)$ 为

$$N_q(n)=\frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d.$$

证 将题 3.4.2 的结论写成 $x^{q^n}-x=\prod_{d|n}\prod_{f(x)\in P_d}f(x)$, 其中 P_d 表示 $F_q[x]$ 中 d 次首 1 不可约多项式的集合. 两边取次数得到 $q^n=\sum_{d|n}dN_q(d)$.

令 $H:\mathbb{N}\longrightarrow\mathbb{Z}$ 为由 $H(n)=q^n$ 给出的映射, $h:\mathbb{N}\longrightarrow\mathbb{Z}$ 为由 $h(n)=nN_q(n)$ 给出的映射, 则由 Möbius 反演律即得

$$nN_q(n)=\sum_{d|n}\mu(d)q^{\frac{n}{d}}=\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d.$$ ■

注 一个自然的问题是: 对于哪些 q 和 n, F_q 上的 n 次首 1 不可约多项式均为本原多项式? 换言之, 对于哪些 q 和 n, q^n 元域 $F_q(u)$ 中的元 u 一定是乘法群 $F_q^*(u)$ 的生成元?

这等价于问: 对于哪些 q 和 n, $N_q(n)=\dfrac{\varphi(q^n-1)}{n}$? 因为 Euler 函数

$$\varphi(m)=m\sum_{d|m}\frac{\mu(d)}{d},$$

故上述问题转化为: 对于哪些 q 和 n,

$$\sum_{d|n}\mu(d)q^{\frac{n}{d}}=(q^n-1)\sum_{d|(q^n-1)}\frac{\mu(d)}{d}?$$

若 $q=2$, $n=p$, 其中 p 为素数, 且 2^p-1 是素数, 则 $F_2[x]$ 中 p 次首 1 不可约多项式必为 $F_2[x]$ 中的 p 次本原多项式. 除此之外, 是否还有这样的情形?

形如 $M_p=2^p-1$ 的数, 其中 p 为素数, 称为 Mersenne 数. 容易证明形如 m^n-1 的素数必为 Mersenne 数, 其中 m,n 均为大于 1 的整数.

§5 有限域上的线性代数

知识要点:

数域上的线性代数可以自然地推广到一般域上. 所以, 也有有限域上的线性代数理论. 由于有限域的特殊性, 有限域上的线性代数产生出新的有趣的现象.

本节内容或许不属于近世代数的经典内容, 希望带动研讨的气氛. 读者可以作更多的探讨.

以下用 F_q 表示 q 元域, 其中 q 为素数的幂.

3.5.1. 以下方阵的集合

$$\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\;\middle|\;a,b,c\in F_q\right\}$$

对于矩阵的乘法作成 q^3 阶非 Abel 群.

证 直接验证. ■

3.5.2*. 求有限域 F_q 上 m $(m\geqslant 1)$ 次一般线性群 $GL_m(F_q)$ 的阶.

解 事实上, F_q 上任一 m 阶矩阵 M 可逆当且仅当其行向量 $\alpha_1,\cdots,\alpha_m$ 是 F_q- 线性无关的, 当且仅当其第一个行向量 $\alpha_1\neq(0,\cdots,0)$ 且第 i 个行向量 α_i 不是前 $i-1$ 个行向量 $\alpha_1,\cdots,\alpha_{i-1}$ 的 F_q- 线性组合, $\forall i,\ 2\leqslant i\leqslant m$.

因此, 可逆矩阵 M 的第一个行向量 α_1 有 q^m-1 种取法 (即 α_1 不能取 $(0,\cdots,0)$); 第二个行向量 α_2 有 q^m-q 种取法 (即 α_2 不能取 $a\alpha_1$, $a\in F_q$); 等等; 第 m 个行向量 α_m 有 q^m-q^{m-1} 种取法 (即 α_m 不能取 $a_1\alpha_1+\cdots+a_{m-1}\alpha_{m-1}$, $a_1,\cdots,a_{m-1}\in F_q$). 从而得到 F_q 上 m 阶可逆矩阵的个数, 也就是一般线性群 $GL_m(F_q)$ 的阶:

$$(q^m-1)(q^m-q)\cdots(q^m-q^{m-1}). \qquad \blacksquare$$

3.5.3*. 求有限域 F_q 上 m $(m\geqslant 2)$ 次特殊线性群 $SL_m(F_q)$ 的阶.

解 考虑由行列式映射给出的群的满同态 $\det: GL_m(F_q)\longrightarrow F_q^*$, 这个满同态的核为 $SL_m(F_q)$. 因此由群同态基本定理知 $F_q^*\cong GL_m(F_q)/SL_m(F_q)$, 从而

$$\frac{|GL_m(F_q)|}{|SL_m(F_q)|}=|F_q^*|=q-1.$$

再由题 3.5.2 的结论即知特殊线性群 $SL_m(F_q)$ 的阶为

$$q^{m-1}(q^m-1)(q^m-q)\cdots(q^m-q^{m-2}). \qquad \blacksquare$$

3.5.4*. 证明有限域 F_q 上 m $(m\geqslant 1)$ 维线性空间 V 有 s 组 (两两不同的) 基, 其中

$$s=\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})}{m!}.$$

证 首先回顾定义: V 的两组基 $v_1,\cdots,v_m$ 和 $u_1,\cdots,u_m$ 称为相同的, 如果作为 V 的子集有 $\{v_1,\cdots,v_m\}=\{u_1,\cdots,u_m\}$.

令

$$\Omega=\{(v_1,\cdots,v_m)\in V\times\cdots\times V\mid v_1,\cdots,v_m \text{ 是 } V \text{ 的一组基}\},$$

则 V 有 s 组 (两两不同的) 基, 其中

$$s=\frac{|\Omega|}{m!}.$$

另一方面, 由线性代数易知 $|\Omega|$ 恰为 F_q 上的 m 阶可逆矩阵的个数. 于是由题 3.5.2 知

$$s=\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})}{m!}. \qquad \blacksquare$$

3.5.5. 有限域 F_{p^n} 作为其子域 F_{p^d} 上的线性空间, 有多少组 (两两不同的) 基?

解　请注意 F_{p^n} 是 F_{p^d} 上的 $m=\dfrac{n}{d}$ 维线性空间. 令 $q=p^d$, 由题 3.5.4 知 F_{p^n} 有

$$s=\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})}{m!}$$

组 (两两不同的) F_{p^d}- 基. ■

3.5.6*. 求证: 有限域 F_q 上 $m\ (m\geqslant 1)$ 维线性空间 V 的 $t\ (1\leqslant t\leqslant m)$ 维子空间的个数为

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}.$$

证　令

$$\Omega_t=\{(w_1,\cdots,w_t)\in V\times\cdots\times V \mid w_1,\cdots,w_t \text{ 是 } F_q\text{- 线性无关的向量}\},$$

并令 Γ_t 是 V 的 t 维子空间的集合. 考虑映射

$$\text{span}:\ \Omega_t\longrightarrow\Gamma_t,$$

对于 $(w_1,\cdots,w_t)\in\Omega_t$, $\text{span}((w_1,\cdots,w_t))$ 定义为以 $w_1,\cdots,w_t$ 为基的 t 维 F_q-线性空间. 显然 span 是满射.

设 $W\in\Gamma_t$, 考虑 W 关于映射 span 的原像的集合 $\text{span}^{-1}(W)$. 由线性代数不难看出 $\text{span}^{-1}(W)$ 恰有 $|GL_t(F_q)|$ 个元. 由题 3.5.2 知

$$|\text{span}^{-1}(W)|=(q^t-1)(q^t-q)\cdots(q^t-q^{t-1}).$$

另一方面, 由线性代数也容易看出 $|\Omega_t|$ 恰为 F_q 上的秩为 t 的 $t\times m$ 矩阵的个数. 按照题 3.5.2 的证明方法可知这个个数为

$$(q^m-1)(q^m-q)\cdots(q^m-q^{t-1}).$$

因为

$$|\Omega_t|=\sum_{W\in\Gamma_t}|\text{span}^{-1}(W)|=|\Gamma_t|(q^t-1)(q^t-q)\cdots(q^t-q^{t-1}),$$

所以

$$|\Gamma_t|=\frac{|\Omega_t|}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}=\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}.$$

这就是所要证明的等式. ■

3.5.7. 设 q 是非零实数且非单位根, 证明

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}=\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{m-t-1})}{(q^{m-t}-1)(q^{m-t}-q)\cdots(q^{m-t}-q^{m-t-1})}.$$

由此即知: 有限域 F_q 上 m $(m\geqslant 1)$ 维线性空间 V 的 t $(1\leqslant t\leqslant m-1)$ 维子空间的个数等于 V 的 $m-t$ 维子空间的个数.

证 将左式的分子分母同乘 t 个 q^{m-t}, 则有

$$\text{左式}=\frac{q^{(m-t)t}(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^m-q^{m-t})(q^m-q^{m-t+1})\cdots(q^m-q^{m-1})};$$

将右式的分子分母同乘 $m-t$ 个 q^t, 则有

$$\text{右式}=\frac{q^{t(m-t)}(q^m-1)(q^m-q)\cdots(q^m-q^{m-t-1})}{(q^m-q^t)(q^m-q^{t+1})\cdots(q^m-q^{m-1})}.$$

现在已经可以看出左式等于右式了.

后一结论由题 3.5.6 即知. ■

3.5.8. 将有限域 F_{q^m} 看成其子域 F_q 上的 m 维线性空间, 则

(1) 有限域 F_{q^m} 有多少个 t $(1\leqslant t\leqslant m)$ 维 F_q- 子空间?

(2) 有限域 F_{q^m} 有多少组含有 t $(1\leqslant t\leqslant m)$ 个元的 F_q- 线性无关向量组?

解 (1) 由题 3.5.6 即知 F_{q^m} 有

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}$$

个 t 维 F_q- 子空间.

(2) 每个 t 维 F_q- 子空间有

$$\frac{|GL_t(F_q)|}{t!}=\frac{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}{t!}$$

组 F_q- 基. 而由 (1) 知 F_{q^m} 有

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}$$

个 t 维 F_q- 子空间, 因此 F_{q^m} 有

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}\frac{(q^t-1)(q^t-q)\cdots(q^t-q^{t-1})}{t!}$$
$$=\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{t-1})}{t!}$$

个含有 t 个 F_q- 线性无关向量的向量组. ■

3.5.9*. 设 G 为 Galois 群 $\mathrm{Gal}(F_{q^n}/F_q)$. 对于每个 $a \in F_{q^n}$, 令

$$T(a) = \sum_{\sigma \in G} \sigma(a), \quad N(a) = \prod_{\sigma \in G} \sigma(a).$$

求证:

(1) $T: F_{q^n} \longrightarrow F_q$ 是 F_q- 线性满射.

(2) $N: F_{q^n}^* \longrightarrow F_q^*$ 是乘法群的满同态.

证 (1) 首先 $\mathrm{Gal}(F_{q^n}/F_q) = \langle \sigma \rangle$ 是 n 阶循环群, 其中 $\sigma(a) = a^q, \forall\, a \in F_{q^n}$. 因此 $T(a) = a + a^q + \cdots + a^{q^{n-1}}$. 因为 $(T(a))^q = T(a)$, 故 $T(a) \in F_q$. 显然 $T: F_{q^n} \longrightarrow F_q$ 是加法群的同态. 又 $T(\lambda a) = \lambda T(a)$, $\forall\, \lambda \in F_q$. 因此 $T: F_{q^n} \longrightarrow F_q$ 是 F_q- 线性映射. 显然, $T \neq 0$ (否则 q^{n-1} 次多项式 $x + x^q + \cdots + x^{q^{n-1}}$ 至少有 q^n 个不同的根. 矛盾!). 而 F_q 是 F_q 上的一维线性空间, 因此 T 必为满射.

(2) 因为 $N(a) = a^{1+q+\cdots+q^{n-1}} = a^{\frac{q^n-1}{q-1}}$, 且 $(N(a))^{q-1} = a^{q^n-1} = 1$, 故 $N(a) \in F_q$. 从而 N 是 $F_{q^n}^*$ 到 F_q^* 的乘法群同态. 设 a 是 $F_{q^n}^*$ 的生成元, 则 a 的乘法阶为 $q^n - 1$, 从而 $N(a)$ 的阶为

$$\frac{q^n - 1}{\left(\frac{q^n-1}{q-1}, q^n - 1\right)} = \frac{q^n - 1}{\frac{q^n-1}{q-1}} = q - 1.$$

而 F_q^* 是 $q-1$ 阶循环群, 故 N 为满同态. ■

3.5.10*. 求群 $G = GL_n(\mathbb{Z}_p)$ 的 Sylow p- 子群的个数.

解 因 $|G| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{\frac{n(n-1)}{2}}(p^n-1)(p^{n-1}-1)\cdots(p-1)$, 故 G 的 Sylow p- 子群的阶为 $p^{\frac{n(n-1)}{2}}$. 令 P 是 G 中对角线为 1 的 n 阶上三角矩阵的集合, 则 P 是 G 的 Sylow p- 子群. 已知 $N_G(P)$ 恰是 G 中上三角矩阵的集合 (参见题 1.3.18), 从而 G 的 Sylow p- 子群的个数为

$$\begin{aligned}[G : N_G(P)] &= \frac{p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1)\cdots(p - 1)}{p^{\frac{n(n-1)}{2}}(p - 1)^n} \\ &= \frac{(p^n - 1)(p^{n-1} - 1)\cdots(p - 1)}{(p - 1)^n}.\end{aligned}$$ ■

3.5.11*. **Dedekind 引理**: 设 E 是任一域, 则 $\mathrm{Aut}(E)$ 的任一有限子集是 E- 线性无关的, 即对于 $\mathrm{Aut}(E)$ 的任一有限子集 Ω, 如果 $\sum_{\sigma \in \Omega} f(\sigma)\sigma = 0$, 其中 $f(\sigma) \in E$, $\forall\, \sigma \in \Omega$, 则 $f(\sigma) = 0$, $\forall\ \sigma \in \Omega$.

将 Dedekind 引理重新表述如下.

Dedekind 引理: 设 E 是任一域, Ω 是 $\mathrm{Aut}(E)$ 的任一有限子集. 设 $f:\Omega\longrightarrow E$ 是一个映射, 满足条件

$$\sum_{\sigma\in\Omega} f(\sigma)\sigma(\alpha)=0,\ \forall\alpha\in E,$$

则 $f(\sigma)=0,\ \forall\sigma\in\Omega$.

证 对 $|\Omega|$ 用数学归纳法. $|\Omega|=1$ 时结论正确, 因为 $\sigma(1)=1\neq 0$.

下设 $|\Omega|>1$. 对任一 $\tau\in\Omega$, $\beta\in E$ 则有

$$\sum_{\sigma\in\Omega} f(\sigma)\sigma(\alpha)\tau(\beta)=0\ ,\ \sum_{\sigma\in\Omega} f(\sigma)\sigma(\alpha)\sigma(\beta)=0\ .$$

两式相减有

$$\sum_{\sigma\in\Omega-\{\tau\}} f(\sigma)(\tau(\beta)-\sigma(\beta))\sigma(\alpha)=0\ ,\forall\alpha\in E\ .$$

由归纳假设即知 $f(\sigma)(\tau(\beta)-\sigma(\beta))=0$, $\forall\sigma\in\Omega-\{\tau\}$. 若存在 $\sigma\in\Omega$, $\sigma\neq\tau$ 使得 $f(\sigma)\neq 0$, 则 $\tau(\beta)=\sigma(\beta)$, $\forall\beta\in E$. 从而 $\sigma=\tau$, 矛盾. 于是 $f(\sigma)=0$, $\forall\sigma\in\Omega-\{\tau\}$. 但 $|\Omega|>1$, τ 任意, 故结论得证. ■

§6 可分扩张

知识要点:

代数扩张 K/F 称为可分扩张, 如果 K 中任一元在 F 上的极小多项式均无重根. 我们基本上只关心可分的域扩张.

域 F 称为完全域, 如果 F 的任一代数扩域均为 F 的可分扩域, 换言之, $F[x]$ 中任一不可约多项式均无重根. 特征为 0 的域是完全域; 特征为素数 p 的域 F 是完全域当且仅当 $F^p=F$, 其中 $F^p=\{a^p\mid a\in F\}$; 有限域是完全域.

有限可分扩张是单扩张.

3.6.1. 设 F 是特征为 0 的域, $f(x)$ 为 $F[x]$ 中正次数首 1 多项式, $d(x)=(f(x),f'(x))$, 其中 $f'(x)$ 是 $f(x)$ 的导数. 求证: $g(x)=f(x)/d(x)$ 和 $f(x)$ 有同样的根, 并且 $g(x)$ 无重根.

证 设 E 是 $f(x)$ 在 F 上的分裂域, 则在 $E(x)$ 中 $f(x)$ 分解为

$$f(x)=(x-x_1)^{r_1}\cdots(x-x_n)^{r_n}\ ,\ r_1,\cdots,\ r_n\geqslant 1,$$

其中 $x_1, \cdots, x_n \in E$ 两两不同. 于是

$$\begin{aligned} f'(x) &= \sum_{1 \leqslant i \leqslant n} r_i(x-x_1)^{r_1} \cdots (x-x_{i-1})^{r_{i-1}}(x-x_i)^{r_i-1}(x-x_{i+1})^{r_{i+1}} \cdots (x-x_n)^{r_n} \\ &= (x-x_1)^{r_1-1} \cdots (x-x_n)^{r_n-1} \sum_{1 \leqslant i \leqslant n} r_i \prod_{j \neq i}(x-x_j). \end{aligned}$$

由此可见在 $E[x]$ 中有 $(f(x), f'(x)) = (x-x_1)^{r_1-1} \cdots (x-x_n)^{r_n-1}$. 而最大公因子不依赖于域 E, 故 $d(x) = (x-x_1)^{r_1-1} \cdots (x-x_n)^{r_n-1} \in F[x]$, $g(x) = (x-x_1) \cdots (x-x_n) \in F[x]$. 由此即可看出所要证明的结论. ■

3.6.2. 设 F 是特征为 p 的域 (p 为素数), $f(x)$ 为 $F[x]$ 中不可约多项式. 求证: $f(x)$ 的所有根均有相同的重数, 且这个公共重数有形式 p^e $(e \geqslant 0)$.

注　本题中若 m 是 $f(x)$ 的互异根的个数 (称之为 $f(x)$ 的简约次数), 则 $\deg f(x) = mp^e$.

证　熟知 $f(x)$ 有重根当且仅当 $(f(x), f'(x)) \neq 1$, 其中 $f'(x)$ 是 $f(x)$ 的形式导数. 因 $f(x)$ 在 F 上不可约, $(f(x), f'(x)) \neq 1$ 当且仅当 $f'(x) = 0$, 当且仅当存在 $g(x) \in F[x]$ 使得 $f(x) = g(x^p)$.

不妨设 $f(x)$ 有重根. 由上段知 $f(x) = g(x^p)$, 且 $g(x)$ 在 $F[x]$ 中也不可约. 若 $g(x)$ 有重根, 重复上段的讨论知 $g(x) = h(x^p)$, 从而 $f(x) = h(x^{p^2})$. 因此 $f(x)$ 总可写成 $f(x) = k(x^{p^e})$, $e > 0$, 其中 $k(x)$ 无重根且不可约. 设 $k(x)$ 在其分裂域上分解为 $k(x) = \prod_{i=1}^{m}(x-x_i)$, 则 $f(x)$ 在其分裂域上分解为

$$f(x) = \prod_{i=1}^{m}(x^{p^e} - x_i) = \prod_{i=1}^{m}(x - \sqrt[p^e]{x_i})^{p^e},$$

从而 $f(x)$ 所有根的重数均为 p^e. ■

3.6.3. 设 F 是特征为 p 的域 (p 为素数), E/F 为代数扩张. 求证: 对每个 $\alpha \in E$ 均存在整数 $n \geqslant 0$, 使得 α^{p^n} 在 F 上可分.

证　设 α 在 F 上的极小多项式是 $f(x)$. 则由题 3.6.2 知 $f(x) = k(x^{p^n})$, 其中 $k(x)$ 是 F 上可分的不可约多项式. 因此 α^{p^n} 在 F 上的极小多项式为 $k(x)$. 从而 α^{p^n} 是 F 上的可分元. ■

3.6.4. 设有域扩张 K/F, $\operatorname{char} F = p$, $\alpha \in K$. 则 α 是 F 上的可分元当且仅当 $F(\alpha) = F(\alpha^p)$.

证　若 α 是 F 上的可分元, 则可断言 $\alpha \in F(\alpha^p)$, 从而 $F(\alpha) = F(\alpha^p)$. 否则 $\alpha \notin F(\alpha^p)$, 于是 α 在 $F(\alpha^p)$ 上的极小多项式为 $x^p - \alpha^p$. 因 α 在 F 上的极小多

项式能被 $x^p - \alpha^p$ 整除, 故 α 在 F 上的极小多项式亦有重根, 这与 α 在 F 上可分相矛盾.

设 $F(\alpha) = F(\alpha^p)$. 若 α 在 F 上不可分, 则 α 在 F 上的极小多项式 $f(x)$ 形如 $f(x) = g(x^p)$, 其中 $g(x)$ 是 $F[x]$ 中不可约多项式. 于是 $g(x)$ 是 α^p 在 F 上的极小多项式, 从而得到矛盾:

$$[F(\alpha^p) : F] = \deg g(x) < \deg f(x) = [F(\alpha) : F] = [F(\alpha^p) : F]. \qquad \blacksquare$$

3.6.5*. 设 α 在 F 上可分, β 在 $F(\alpha)$ 上可分, 则 β 在 F 上可分.

证 不妨设 $\mathrm{char}\, F = p$, 根据题 3.6.4 只要证 $F(\beta) = F(\beta^p)$.

设 α 在 $F(\beta)$ 上的极小多项式为 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, 其中 $a_i \in F(\beta), i = 0, 1, \cdots, n-1$. 则 $f^p(x) \in F(\beta^p)[x]$, $f^p(\alpha) = 0$. 于是 α 在 $F(\beta^p)$ 上的极小多项式 $g(x)$ 整除 $f^p(x)$, 且在 $F(\beta)[x]$ 中有 $f(x) \mid g(x) \mid f^p(x)$. 因 $f(x)$ 在 $F(\beta)[x]$ 中不可约, 从而 $g(x) = f^t(x)$. 但 α 在 $F(\beta^p)$ 上可分, 所以只能 $f(x) = g(x)$. 故有

$$[F(\beta)(\alpha) : F(\beta)] = \deg f(x) = \deg g(x) = [F(\beta^p)(\alpha) : F(\beta^p)].$$

因 β 在 $F(\alpha)$ 上可分, 由题 3.6.4 知 $F(\alpha)(\beta) = F(\alpha)(\beta^p)$, 从而 $F(\beta) = F(\beta^p)$. 证毕. $\blacksquare$

3.6.6*. (1) 设 E/F 为代数扩张, S 是 E 的子集. 证明: $F(S)/F$ 是可分扩张当且仅当 S 中元在 F 上都是可分的.

(2) 若 α, β 在 F 上可分, 则 $\alpha \pm \beta, \alpha\beta, \dfrac{\alpha}{\beta}$ $(\beta \neq 0)$ 均在 F 上可分.

(3) F 上可分多项式在 F 上的分裂域在 F 上可分.

(4) 若 E/K 和 K/F 为可分扩张, 则 E/F 为可分扩张; 反之亦然.

证 (1) 设 S 中元在 F 上都是可分的. 设 $\alpha \in F(S)$, 则存在 $u_1, \cdots, u_m \in S$ 使得 $\alpha \in F(u_1, \cdots, u_m)$. 因 u_m 在 $F(u_1, \cdots, u_{m-1})$ 上可分, α 在 $F(u_1, \cdots, u_{m-1})(u_m)$ 上可分, 由题 3.6.5 即知 α 在 $F(u_1, \cdots, u_{m-1})$ 上可分. 重复这一证明最后逐步得到 α 在 F 上可分.

(2) 和 (3) 是 (1) 的直接推论.

(4) 设 $\alpha \in E$. 设 α 在 K 上的极小多项式为 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, 则 α 在 $F(a_0, \cdots, a_{n-1}) = F(a_0, \cdots, a_{n-2})(a_{n-1})$ 上可分, 由 (1) 知 $F(a_0, \cdots, a_{n-1})/F$ 为可分扩张, 特别地, a_{n-1} 在 $F(a_0, \cdots, a_{n-2})$ 上可分. 故由题 3.6.5 知 α 在 $F(a_0, \cdots, a_{n-2})$ 上可分. 重复这一证明最后逐步得到 α 在 F 上可分.

反之是容易的. 设 E/F 为可分扩张. 设 $\alpha \in E$, $p(x)$ 和 $q(x)$ 分别是 α 在 F 上和在 K 上的极小多项式, 则 $q(x)|p(x)$. 因为 $p(x)$ 无重根, 故 $q(x)$ 无重根, 即 E/K 可分. 因 $K \subseteq E$, E/F 是可分扩张, 由定义知 K/F 是可分扩张. ■

3.6.7*. **同构延拓定理的强形式** 设 $\sigma: F \longrightarrow F'$ 是域同构, $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ 是 $F[x]$ 中的正次数多项式, E 和 E' 分别是 $f(x)$ 在 F 上和 $f^\sigma(x) = \sigma(a_n)x^n + \sigma(a_{n-1})x^{n-1} + \cdots + \sigma(a_1)x + \sigma(a_0)$ 在 F' 上的分裂域. 则 σ 可延拓成域同构 $E \longrightarrow E'$; 这种延拓的个数 m 满足 $1 \leqslant m \leqslant [E:F]$.

而且 $m = [E:F]$ 当且仅当 $f(x)$ 是 F 上的可分多项式.

证 注意到 $f(x)$ 是 F 上的可分多项式当且仅当 $f^\sigma(x)$ 是 F' 上的可分多项式.

对 $[E:F]$ 用数学归纳法. 若 $[E:F] = 1$, 则 $E = F$, $E' = F'$. 结论自然成立. 设 $[E:F] < n$ 时结论成立. 现设 $[E:F] = n \geqslant 2$, 因此 $f(x)$ 有次数 d 大于 1 的首 1 不可约因子 $g(x) \in F[x]$. 设 u 是 $g(x)$ 在 E 中的一个根, 则 σ 共有 t 个延拓 $\sigma_1, \cdots, \sigma_t$: $F(u) \longrightarrow E'$, 它们均为域嵌入, 其中 t 等于 $g^\sigma(x) \in F'[x]$ 在 E' 中互异根的个数. 因此 $1 \leqslant t \leqslant d$; 并且 $t = d$ 当且仅当 $g^\sigma(x)$ 是 F' 上的可分多项式, 当且仅当 $g(x)$ 是 F 上的可分多项式.

对于每一域同构 σ_i: $F(u) \longrightarrow F'(u_i)$, E 和 E' 分别是 $f(x)$ 在 $F(u)$ 上和 $f^\sigma(x)$ 在 $F'(u_i)$ 上的分裂域, 其中 $u_i := \sigma_i(u) \in E'$. 因为 $[E:F(u)] < [E:F] = n$, 由归纳假设知 σ_i 可延拓成域同构 $E \longrightarrow E'$, 这种延拓的个数 m_i 满足 $1 \leqslant m_i \leqslant [E:F(u)]$; 进而, $m_i = [E:F(u)]$ 当且仅当 $f(x)$ 是 $F(u)$ 上的可分多项式.

于是, 以上述方式我们得到 σ 的 m 个不同的延拓 $E \longrightarrow E'$, 其中

$$1 \leqslant m = \sum_{1\leqslant i\leqslant t} m_i \leqslant t[E:F(u)] \leqslant d[E:F(u)] = [F(u):F][E:F(u)] = [E:F];$$

进而, $m = [E:F]$ 当且仅当 $t = d$ 且 $m_i = [F:F(u)]$, $1 \leqslant i \leqslant t$; 当且仅当 $g(x)$ 是 F 上的可分多项式并且 $f(x)$ 是 $F(u)$ 上的可分多项式. 换言之, 这当且仅当 u 是 F 上的可分元并且 $f(x)$ 的任意根是 $F(u)$ 上的可分元; 由题 3.6.5 知这当且仅当 $f(x)$ 的任意根是 F 上的可分元, 即 $f(x)$ 是 F 上的可分多项式.

现在, 设域同构 $\phi: E \longrightarrow E'$ 是 σ 的一个延拓, 则 ϕ 在 $F(u)$ 上的限制是域嵌入 $F(u) \longrightarrow E'$ 且是 σ 的一个延拓. 因此这个限制是某一 σ_i, 从而 ϕ 是 σ_i 的一个延拓, 因此 ϕ 已经包含在上述 m 个 σ 的延拓之列. 证毕. ■

3.6.8. 设 $E = F_p(x, y)$, $F = F_p(x^p,\ y^p)$, 其中 F_p 为 p 元域, x, y 是 F_p 上的超越元. 求证:

(1) $[E:F]=p^2$.

(2) E/F 不是单扩张.

(3) E/F 有无限多个中间域.

证 (1) $[E:F]=[F_p(x,y):F_p(x^p,y^p)]=[F_p(x,y):F_p(x,y^p)][F_p(y^p,x):F_p(y^p,x^p)]=p\cdot p=p^2$.

(2) 若 E/F 是单扩张, 即 $E=F(\mu)$, 则 μ 在 F 上的极小多项式 $p(t)$ 是 p^2 次的. 因为 E/F 不是可分扩域, 故 μ 不是 F 上可分元, 即 $p(t)$ 有重根. 因此由题 3.6.2 知 $p(t)=k(t^{p^2})$ 或 $p(t)=k(t^p)$, 其中 $k(t)$ 是 F 上无重根不可约多项式. 因 $F_p^p=F_p$, 故 $F^p=F$. 因此无论 $p(t)=k(t^{p^2})$ 或 $p(t)=k(t^p)$, 均有 $p(t)=h^p(t)$, $h(t)\in F[t]$. 这与 $p(t)$ 在 F 上不可约相矛盾! 这表明 E/F 不是单扩张.

(3) 令 $M_b=F(x+by)$, $b\in F$, 则 M_b 是 E/F 的中间域. 若 $M_a=M_b$, $a\neq b$, 则 $x+ay\in F(x+by)$. 从而 $y\in F(x+by)$, 进而 $x\in F(x+by)$. 于是 $E=F(x+by)$ 是单扩域, 矛盾! 因 F 是无限域, 故 E/F 有无限多个中间域 M_b. ■

3.6.9. (1) 若 E/F 为代数扩张, F 为完全域, 则 E 也为完全域.

(2) 若 E/F 为单扩张 (不必为代数扩张), E 为完全域, 问 F 是否也为完全域?

(3) 若 E/F 为有限生成扩张 (不必为代数扩张), E 为完全域, 问 F 是否也为完全域?

(4) 若 E/F 为有限扩张, E 为完全域, 问 F 是否也为完全域?

(5) 若 E/F 为代数扩张 (不必为有限扩张), E 为完全域, 问 F 是否也为完全域?

证 (1) 否则, 设 $E[x]$ 中有不可约多项式 $p(x)$, $p(x)$ 有重根 α. 因 E/F 是代数扩张, α 在 E 上代数, 故 α 在 F 上代数. 设 $q(x)$ 是 α 在 F 上的极小多项式, 则 $p(x)|q(x)$, 从而 $q(x)$ 也有重根. 这与 F 是完全域不合.

(2) 是. 不妨设 $\operatorname{char}F=p>0$. 设 $E=F(\alpha)$, 因为 E 完全, $E^p=E$, 故 $\alpha\in E^p=F^p(\alpha^p)$. 因此 α 在 F^p 上代数 (参见题 3.1.6), 故 α 在 F 上代数.

欲证 F 完全, 只要证 $F=F^p$, 只要证 $[F(\alpha):F^p]=[F(\alpha):F]$, 或等价地, $[F(\alpha):F^p]\leqslant[F(\alpha):F]$.

由于 $E=F(\alpha)$ 是完全域, 故 $E^p=E$. 注意到 $E^p=F^p(\alpha^p)$, 因此只要证 $[F^p(\alpha^p):F^p]\leqslant[F(\alpha):F]$, 而这是对的. 事实上, 设 α 在 F 上的极小多项式为 $f(x)=a_0+a_1x+\cdots+a_nx^n$, 则 α^p 是 F^p 上的多项式 $g(x)=a_0^p+a_1^px+\cdots+a_n^px^n$ 的根.

(3) 是. 不妨设 $\operatorname{char}F=p>0$, $E=F(\alpha_1,\cdots,\alpha_n)$. 对 n 用数学归纳

法. 当 $n=1$ 时由本题 (2) 知结论成立. 设 $n>1$, 则 $E=F(\alpha_1,\cdots,\alpha_n)$ 是 $F(\alpha_1,\cdots,\alpha_{n-1})$ 的单扩域. 由本题 (2) 知 $F(\alpha_1,\cdots,\alpha_{n-1})$ 是完全域. 再由归纳假设知 F 是完全域.

(4) 有限扩张当然是有限生成扩张, 故由 (3) 知 F 是完全域.

(5) 否.

令 $F=F_p(t)$, 其中 F_p 为 p 元域, t 是 F_p 上的超越元, 则 $x^p-t\in F[x]$ 是 F 上的有重根不可约多项式. 故 F 不是完全域.

令 $p_n(x)=x^{p^n}-t\in F[x]$, E 是 $\{p_n(x)\mid n=0,1,2,\cdots\}$ 在 F 上的分裂域. 则 E/F 是代数扩张. 但 E 是完全域, 这是因为 $E^p=E$.

这表明当 E/F 是代数扩张, E 是完全域时, F 未必是完全域. ■

§7 正规扩张

知识要点:

代数扩张 K/F 称为正规扩张, 如果在 K 中有根的 $F[x]$ 中不可约多项式的全部根均在 K 中; 换言之, 如果 K 中任一元在 F 上的极小多项式的根均在 K 中.

K/F 是有限正规扩域当且仅当 K 是 $F[x]$ 中某一多项式的分裂域.

可分正规扩域 K/F 称为 Galois 扩域. K/F 是有限 Galois 扩域当且仅当 K 是 $F[x]$ 中某一可分多项式的分裂域.

有限 Galois 扩域 E/F 必是单扩域; 其 Galois 群 $\mathrm{Gal}(E/F)$ 的阶恰为 $[E:F]$.

3.7.1. 设 $E=\mathbb{Q}(\alpha)$, 其中 $\alpha^3+\alpha^2-2\alpha-1=0$. 求证:

(1) α^2-2 也是 $x^3+x^2-2x-1=0$ 的根.

(2) $E/\mathbb{Q}$ 是正规扩张.

证 $\alpha^3=-\alpha^2+2\alpha+1$, $\alpha^4=-\alpha^3+2\alpha^2+\alpha=3\alpha^2-\alpha-1$,

$$(\alpha^2-2)^3+(\alpha^2-2)^2-2(\alpha^2-2)-1=(\alpha^2-2)[(\alpha^2-2)^2+(\alpha^2-2)-2]-1$$
$$=(\alpha^2-2)(\alpha^4-3\alpha^2)-1=-(\alpha^2-2)(\alpha+1)-1=-(\alpha^3+\alpha^2-2\alpha-1)=0,$$

因此 x^3+x^2-2x-1 的三个根均属于 E (事实上, $\dfrac{x^3+x^2-2x-1}{(x-\alpha)(x-\alpha^2+2)}=x+(\alpha^2+\alpha-1)$, x^3+x^2-2x-1 的三个根为 $\alpha,\alpha^2-2,-\alpha^2-\alpha+1$), 从而 E 是 x^3+x^2-2x-1 在 $\mathbb{Q}$ 上的分裂域, 故 $E/\mathbb{Q}$ 是正规扩张. ■

3.7.2. 设 E/F 和 K/F 均是正规扩张, 求证: EK/F 也是正规扩张.

证 因 E/F 和 K/F 均是正规扩张, 故 E 和 K 分别是 $F[x]$ 中某个多项式集合 S 和 T 在 F 上的分裂域, 从而 EK 是 $F[x]$ 中多项式集合 $S\bigcup T$ 在 F 上的分裂域. 故 EK/F 是正规扩张. ■

3.7.3. 域的二次扩张 E/F 必是正规扩张. 试决定二次扩张的 Galois 群.

证 设 $[E:F]=2$, 则 $E=F(\nu)$, $\nu\notin F$. 设 ν 在 F 上的极小多项式为 $f(x)=x^2+ax+b$, 则 $f(x)$ 的另一根为 $-(a+\nu)$. 故 E 是 $f(x)$ 在 F 上的分裂域, 从而 E/F 正规.

因 $f(x)$ 无重根 (否则 $f'(x)=0$. 从而 $\mathrm{char}F=2$, $a=0$. 于是 $f(x)=x^2+1=(x+1)^2$ 可约, 矛盾), 故 $\mathrm{Gal}(E/F)$ 是 2 阶循环群, 其生成元 σ 将 ν 送到 $-(a+\nu)$. ■

3.7.4. (1) 如果 E/M 和 M/F 均是域的正规扩张, 试问 E/F 是否一定为正规扩张?

(2) 如果 E/F 是正规扩张, M 是它们的中间域, 试问 E/M 和 M/F 是否一定为正规扩张?

证 (1) 否. 例如, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 和 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ 均正规, 但 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不正规. 这是因为不可约多项式 $f(x)=x^4-2\in\mathbb{Q}[x]$ 有一根 $\sqrt[4]{2}$ 属于 $\mathbb{Q}(\sqrt[4]{2})$, 但 $f(x)$ 的根 $\sqrt[4]{2}\mathrm{i}\notin\mathbb{Q}(\sqrt[4]{2})$.

(2) 设 E/F 正规, M 是中间域. 则 E 是 $F[x]$ 中某个多项式集合 S 在 F 上的分裂域, 从而 E 也是 $M[x]$ 中多项式集合 S 在 M 上的分裂域, 故 E/M 也正规.

但 M/F 未必正规. 例如, $E=\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ 是正规扩张, $\omega=\mathrm{e}^{\frac{2\pi}{3}\mathrm{i}}$, $M=\mathbb{Q}(\sqrt[3]{2})$ 是中间域, 但 $M/\mathbb{Q}$ 不是正规扩张. ■

3.7.5*. 设 E/F 为有限代数扩张. 求证: E/F 为正规扩张 $\Longleftrightarrow$ 对于 $F[x]$ 中任意不可约多项式 $f(x)$, $f(x)$ 在 $E[x]$ 中的所有不可约因子均有相同的次数.

证 $\Longleftarrow$: 设 $f(x)$ 是 $F[x]$ 中不可约多项式且有一个根在 E 中. 则 $f(x)$ 在 $E[x]$ 中有一次因子. 故由假设 $f(x)$ 在 $E[x]$ 中的所有不可约因子均是一次的, 即 $f(x)$ 的所有根均在 E 中, 即 E/F 是正规扩张.

$\Longrightarrow$: 设 E/F 是有限正规扩张. 则 E 是 F 上某个多项式 $g(x)$ 在 F 上的分裂域.

设 $f(x)$ 是 $F[x]$ 中任一不可约多项式, $p(x)$ 和 $q(x)$ 是 $f(x)$ 在 $E[x]$ 中的两个首 1 的不可约因子. 令 M 是 $f(x)$ 在 F 上的分裂域. 设 α, $\beta\in M$, 使得 $p(\alpha)=0=q(\beta)$. 因为 α, β 在 F 上的极小多项式均为 $f(x)$, 故存在域同构 $\eta:\ F(\alpha)\longrightarrow F(\beta)$, $\eta|_F=\mathrm{id}$, $\eta(\alpha)=\beta$. 因 M 是 $f(x)$ 在 $F(\alpha)$ 上的分裂域, 也是 $f(x)$ 在 $F(\beta)$ 上的分裂域, 故由同构延拓定理知, η 可延拓为 $\tau:\ M\longrightarrow M$, $\tau|_{F(\alpha)}=\eta$.

现在 EM 是 M 上多项式 $g(x)$ 在 M 上的分裂域. 注意此处总可将 E, M 视为某一共同域的子域, 例如 F 的代数闭包. 因此由同构延拓定理, τ 可延拓为

$\xi: EM \longrightarrow EM$, $\xi|_M = \tau$.

由于 E/F 正规, $\xi|_F = \mathrm{id}$, 故 $\xi(E) = E$. ξ 将 $p(x) \in E[x]$ 仍变成 $E[x]$ 中的不可约多项式, 由于 $\xi(\alpha) = \beta$, 故 $\xi(p(x))$ 与 $q(x)$ 均为 $E[x]$ 中以 β 为零点的不可约多项式. 从而 $\xi(p(x)) = q(x)$. 特别地, $p(x)$ 与 $q(x)$ 的次数相同. ■

3.7.6*. 设 E/F 为有限正规扩张, $G = \mathrm{Gal}(E/F)$, M 是 E/F 的中间域. 则 M/F 是正规扩张当且仅当 $\sigma(M) = M$, $\forall\, \sigma \in G$.

证 $\Longrightarrow$: 设 M/F 是正规扩张. 则 M 是 $F[x]$ 中某一多项式 $f(x)$ 在 F 上的分裂域. 故 $M = F(\alpha_1, \cdots, \alpha_m)$, 其中 $\alpha_1, \cdots, \alpha_m$ 是 $f(x)$ 的全部两两不同的根 (若 $f(x)$ 有重根, 则每个重根只取一次). 则 G 中任一元 σ 在 $\alpha_1, \cdots, \alpha_m$ 上的作用是 $\alpha_1, \cdots, \alpha_m$ 的一个置换. 因此 $\sigma(M) = M$.

$\Longleftarrow$: 反之, 设 $\sigma(M) = M$, $\forall\, \sigma \in G$. 设 $\alpha \in M$, $g(x)$ 是 α 在 F 上的极小多项式. 设 β 是 $g(x)$ 的任一根, 则存在域同构 $\tau:\ F(\alpha) \longrightarrow F(\beta)$, $\tau|_F = \mathrm{id}$, $\tau(\alpha) = \beta$.

因为 E/F 为有限正规扩张, 故 E 是 F 上某个多项式 $f(x)$ 在 F 上的分裂域. 从而 $E(\alpha)$ 是 $f(x)$ 在 $F(\alpha)$ 上的分裂域, $E(\beta)$ 是 $f(x)$ 在 $F(\beta)$ 上的分裂域. 由同构延拓定理, τ 可延拓为域同构 $\sigma: E(\alpha) \longrightarrow E(\beta)$. 因 $\alpha \in M$, 故 $\alpha \in E$; 又因 E/F 正规, 故 $\beta \in E$. 从而 $E(\alpha) = E = E(\beta)$, $\sigma \in G$. 于是 $\beta = \tau(\alpha) = \sigma(\alpha) \in \sigma(M) = M$. 这就证明了 M/F 是正规扩张. ■

第 4 章　Galois 理论

§1　基 本 定 理

知识要点:

Galois 理论的基本定理揭示了群和域之间存在的反序一一对应. 确切地说, 设 E/F 是有限 Galois 扩张, $G = \mathrm{Gal}(E/F) = \{\ \sigma:\ E \longrightarrow E$ 是域同构 $\mid \sigma(a) = a,\ \forall\ a \in F\ \}$. 令 $\Omega = \{\ E/F$ 的中间域$\}, \Gamma = \{\ G$ 的子群 $\}$. 考虑如下两个映射:

$$\mathrm{Gal}(E/-):\ \Omega \longrightarrow \Gamma,\quad \text{其中}\quad \mathrm{Gal}(E/-)(M) = \mathrm{Gal}(E/M),\quad \forall\ M \in \Omega,$$

$$\mathrm{Inv}:\ \Gamma \longrightarrow \Omega,\quad \text{其中}\quad \mathrm{Inv}(H) = \{\ a \in E \mid \sigma(a) = a,\ \forall\ \sigma \in H\ \}, \forall H \in \Gamma.$$

注意到 E/M 也是有限 Galois 扩张, $\forall\ M \in \Omega$. 从而有

$$[E:M] = |\,\mathrm{Gal}(E/M)|,\quad [M:F] = [G:\mathrm{Gal}(E/M)],\quad \forall\ M \in \Omega.$$

Galois 理论的基本定理 (主要) 是说:

(1)　$\mathrm{Gal}(E/-):\ \Omega \longrightarrow \Gamma$　和 $\mathrm{Inv}:\ \Gamma \longrightarrow \Omega$ 是互逆的反序的映射. 于是有

$$\mathrm{Inv}(\mathrm{Gal}(E/M)) = M,\quad \mathrm{Gal}(E/\mathrm{Inv}(H)) = H,\quad \forall\ M \in \Omega,\quad \forall\ H \in \Gamma;$$

$$[E:\mathrm{Inv}(H)] = |H|,\quad [\mathrm{Inv}(H):F] = [G:H],\quad \forall\ H \in \Gamma.$$

(2)　H 是 G 的正规子群当且仅当 $\mathrm{Inv}(H)/F$ 是正规扩张; 或等价地, M/F 是正规扩张当且仅当 $\mathrm{Gal}(E/M)$ 是 G 的正规子群. 在这种情况下, 有

$$\mathrm{Gal}(\mathrm{Inv}(H)/F) \cong G/H;$$

或等价地,

$$\mathrm{Gal}(M/F) \cong G/\mathrm{Gal}(E/M).$$

这条基本定理的证明所需的知识点在以前相关章节的“知识要点”中都已提到, 除了下面的 Artin 引理.

Artin 引理:　设 K 是域, G 是 K 的自同构群 $\mathrm{Aut}(K)$ 的有限子群. 则有 $[K:\mathrm{Inv}(G)] \leqslant |G|$,　这里 $\mathrm{Inv}(G) = \{\ a \in K \mid \sigma(a) = a,\ \forall\ \sigma \in G\ \}$.

Galois 理论的基本定理很重要, 且其证明值得回顾. 我们首先以习题的形式包含这个证明.

在以下习题 4.1.1—4.1.3 中, E/F, G, Ω, Γ, M, H, $\mathrm{Gal}(E/M)$, $\mathrm{Inv}(H)$ 意思同上.

4.1.1. 求证: (1) $\mathrm{Gal}(E/-): \ \Omega \longrightarrow \Gamma$ 和 $\mathrm{Inv}: \ \Gamma \longrightarrow \Omega$ 是反序的映射, 即若 $M_1 \subseteq M_2$, 则 $\mathrm{Gal}(E/M_1) \supseteq \mathrm{Gal}(E/M_2)$; 若 $H_1 \subseteq H_2$, 则 $\mathrm{Inv}(H_1) \supseteq \mathrm{Inv}(H_2)$.

(2) (作用 3 次等于作用 1 次) 对于 $M \in \Omega$, $H \in \Gamma$ 有

$$\mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/M))) = \mathrm{Gal}(E/M), \quad \mathrm{Inv}(\mathrm{Gal}(E/\mathrm{Inv}(H))) = \mathrm{Inv}(H).$$

证 (1) 映射 $\mathrm{Gal}(E/-)$ 和 Inv 的反序性由定义直接可得.

(2) 由定义有 $M \subseteq \mathrm{Inv}(\mathrm{Gal}(E/M))$; 由映射 $\mathrm{Gal}(E/-)$ 的反序性得到

$$\mathrm{Gal}(E/M) \supseteq \mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/M))).$$

记 $H = \mathrm{Gal}(E/M) \leqslant G$. 又由定义知 $H \subseteq \mathrm{Gal}(E/\mathrm{Inv}(H))$, 即

$$\mathrm{Gal}(E/M) \subseteq \mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/M))).$$

所以 $\mathrm{Gal}(E/M) = \mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/M)))$.

同理可证另一式. ■

4.1.2*. 证明 Artin 引理: 设 K 是域, G 是 K 的自同构群 $\mathrm{Aut}(K)$ 的有限子群. 则有 $[K:\mathrm{Inv}(G)] \leqslant |G|$, 这里 $\mathrm{Inv}(G) = \{\, a \in K \mid \sigma(a) = a, \ \forall\, \sigma \in G \,\}$.

证 设 $|G| = n$. 不妨设 $n > 1$, 欲证 $[K:\mathrm{Inv}(G)] \leqslant n$, 只要证 K 中任意 $n+1$ 个元 $u_1, \cdots, u_{n+1}$ 必然 $\mathrm{Inv}(G)$- 线性相关. 记 $G = \{f_1, \cdots, f_n\}$, 其中 $f_1 = \mathrm{id}_K$. 取 K 上 $n+1$ 个变量、n 个方程的齐次线性方程组

$$\sum_{1 \leqslant j \leqslant n+1} f_i(u_j)x_j = 0, \ 1 \leqslant i \leqslant n \tag{$*$}$$

的非零解 $(a_1, \cdots, a_{n+1})$, 使得 $(a_1, \cdots, a_{n+1})$ 在方程组 $(*)$ 的所有非零解中非零分量的个数最少. 必要时调换 u_j 和 x_j 的下标, 不妨设 $a_1 \neq 0$; 进而, 不妨设 $a_1 = 1$.

我们断言: $a_j \in \mathrm{Inv}(G)$, $1 \leqslant j \leqslant n+1$. 从而由方程组 $(*)$ 的第一个方程知

$$\sum_{1 \leqslant j \leqslant n+1} u_j a_j = 0,$$

因 $a_1 = 1$, 这表明 $u_1, \cdots, u_{n+1}$ 是 $\mathrm{Inv}(G)$- 线性相关的.

如果断言不成立, 不妨设 $a_2 \notin \mathrm{Inv}(G)$. 则有 $2 \leqslant t \leqslant n$ 使得 $f_t(a_2) \neq a_2$. 将 f_t 作用在方程组 $(*)$ 上得到

$$\sum_{1 \leqslant j \leqslant n+1} f_t f_i(u_j) f_t(a_j) = 0, \ 1 \leqslant i \leqslant n.$$

因 G 是群, 故 $f_t f_1, \cdots, f_t f_n$ 是 $f_1, \cdots, f_n$ 的一个置换, 从而 $(f_t(a_1) = 1, f_t(a_2), \cdots, f_t(a_{n+1}))$ 是方程组 $(*)$ 的解. 于是

$$(0, a_2 - f_t(a_2), \cdots, a_{n+1} - f_t(a_{n+1}))$$

也是方程组 $(*)$ 的解. 因 $f_t(a_2) \neq a_2$, 上述解是方程组 $(*)$ 的非零解, 而且其非零分量的个数比 $(1, a_2, \cdots, a_{n+1})$ 的非零分量的个数要少, 这与 $(1, a_2, \cdots, a_{n+1})$ 的取法相矛盾! 证毕! ■

4.1.3*. 证明 Galois 理论基本定理:

(1) $\mathrm{Gal}(E/-): \ \Omega \longrightarrow \Gamma$ 和 $\mathrm{Inv}: \ \Gamma \longrightarrow \Omega$ 是互逆的反序的映射.

(2) H 是 G 的正规子群当且仅当 $\mathrm{Inv}(H)/F$ 是正规扩张. 在这种情况下, 有

$$\mathrm{Gal}(\mathrm{Inv}(H)/F) \cong G/H.$$

证 (1) 由定义有 $M \subseteq \mathrm{Inv}(\mathrm{Gal}(E/M))$. 因 $E/\mathrm{Inv}(\mathrm{Gal}(E/M))$ 和 E/M 均是有限 Galois 扩张, 故

$$[E : \mathrm{Inv}(\mathrm{Gal}(E/M))] = |\mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/M)))| = |\mathrm{Gal}(E/M)| = [E : M],$$

其中第二个等式由题 4.1.1(2) 得出. 由此即得 $M = \mathrm{Inv}(\mathrm{Gal}(E/M))$.

由定义有 $H \subseteq \mathrm{Gal}(E/\mathrm{Inv}(H))$. 因 $E/\mathrm{Inv}(H)$ 是有限 Galois 扩张, 故

$$[E : \mathrm{Inv}(H)] = |\mathrm{Gal}(E/\mathrm{Inv}(H))| \geqslant |H|.$$

从而

$$|H| \leqslant |\mathrm{Gal}(E/\mathrm{Inv}(H))| = [E : \mathrm{Inv}(H)] \leqslant |H|,$$

其中第二个不等式由 Artin 引理得出. 于是 $\mathrm{Gal}(E/\mathrm{Inv}(H)) = H$.

(2) H 是 G 的正规子群当且仅当 $\sigma H \sigma^{-1} = H, \ \forall\, \sigma \in G$; 由 (1) 知当且仅当 $\mathrm{Inv}(\sigma H \sigma^{-1}) = \mathrm{Inv}(H), \ \forall\, \sigma \in G$. 而

$$\begin{aligned}
\mathrm{Inv}(\sigma H \sigma^{-1}) &= \{a \in E \mid \sigma h \sigma^{-1}(a) = a, \ \forall\, h \in H\} \\
&= \{a \in E \mid h\sigma^{-1}(a) = \sigma^{-1}(a), \ \forall\, h \in H\} \\
&= \{a \in E \mid \sigma^{-1}(a) \in \mathrm{Inv}(H)\} \\
&= \sigma(\mathrm{Inv}(H)).
\end{aligned}$$

因此, $H \lhd G$ 当且仅当 $\mathrm{Inv}(H) = \sigma(\mathrm{Inv}(H)), \ \forall\, \sigma \in G$; 根据题 3.7.6, 这当且仅当 $\mathrm{Inv}(H)$ 是 F 的正规扩域.

设 H 是 G 的正规子群. 因为 $\sigma(\mathrm{Inv}(H)) = \mathrm{Inv}(H)$, $\forall\, \sigma \in G$, 故有映射

$$\pi:\ G \longrightarrow \mathrm{Gal}(\mathrm{Inv}(H)/F),\quad \sigma \mapsto \sigma|_{\mathrm{Inv}(H)}.$$

显然 π 是群的同态, 且

$$\mathrm{Ker}\,\pi = \{\, \sigma \in G \mid \sigma|_{\mathrm{Inv}(H)} = \mathrm{id}_{\mathrm{Inv}(H)}\} = \mathrm{Gal}(E/\,\mathrm{Inv}(H)) = H.$$

于是 π 诱导出群的单同态

$$G/H \longrightarrow \mathrm{Gal}(\mathrm{Inv}(H)/F).$$

因 $\mathrm{Inv}(H)$ 是 F 的正规扩域, 故

$$|\,\mathrm{Gal}(\mathrm{Inv}(H)/F)| = [\mathrm{Inv}(H):F] = \frac{[E:F]}{[E:\mathrm{Inv}(H)]} = \frac{|G|}{|\,\mathrm{Gal}(E/\,\mathrm{Inv}(H))|} = \frac{|G|}{|H|},$$

从而上述单同态是群同构. 这就完成了证明. ■

4.1.4. 设 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, u)$, $u^2 = (9-5\sqrt{3})(2-\sqrt{2})$. 求证 $E/\mathbb{Q}$ 是 Galois 扩张, 并决定 Galois 群 $\mathrm{Gal}(E/\mathbb{Q})$.

证　因 $\mathbb{Q}$ 特征为零, 故 $E/\mathbb{Q}$ 是可分扩域. 设 Ω 是 E 的代数闭包, $\sigma:\ E \longrightarrow \Omega$ 是域的嵌入. 则 $\sigma|_{\mathbb{Q}} = \mathrm{id}$, $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$. 从而 $\sigma(u^2) = u^2$, 或

$$\sigma(u^2) = (9+5\sqrt{3})(2-\sqrt{2}) = \frac{(9+5\sqrt{3})^2}{6}u^2,$$

或

$$\sigma(u^2) = (9-5\sqrt{3})(2+\sqrt{2}) = \frac{(2+\sqrt{2})^2}{2}u^2,$$

或

$$\sigma(u^2) = (9+5\sqrt{3})(2+\sqrt{2}) = \frac{(9+5\sqrt{3})^2(2+\sqrt{2})^2}{12}u^2.$$

于是

$$\sigma(u) = \pm u,\ \text{或}\ \sigma(u) = \pm\frac{9+5\sqrt{3}}{\sqrt{6}}u,\ \text{或}\ \sigma(u) = \pm(1+\sqrt{2})u,$$

$$\text{或}\ \sigma(u) = \pm\frac{(2+\sqrt{2})(9+5\sqrt{3})}{2\sqrt{3}}u.$$

总之 $\sigma(u) \in E$. 这表明 $E/\mathbb{Q}$ 是正规扩域, 从而 $E/\mathbb{Q}$ 是 8 次 Galois 扩域, 且

$|\mathrm{Gal}(E/\mathbb{Q})| = 8$. 令

$$\sigma_1 = \mathrm{id};$$
$$\sigma_2(\sqrt{2}) = \sqrt{2}, \quad \sigma_2(\sqrt{3}) = \sqrt{3}, \quad \sigma_2(u) = -u;$$
$$\sigma_3(\sqrt{2}) = -\sqrt{2}, \quad \sigma_3(\sqrt{3}) = \sqrt{3}, \quad \sigma_3(u) = (1+\sqrt{2})u;$$
$$\sigma_4(\sqrt{2}) = -\sqrt{2}, \quad \sigma_4(\sqrt{3}) = \sqrt{3}, \quad \sigma_4(u) = -(1+\sqrt{2})u;$$
$$\sigma_5(\sqrt{2}) = \sqrt{2}, \quad \sigma_5(\sqrt{3}) = -\sqrt{3}, \quad \sigma_5(u) = \frac{9+5\sqrt{3}}{\sqrt{6}}u;$$
$$\sigma_6(\sqrt{2}) = \sqrt{2}, \quad \sigma_6(\sqrt{3}) = -\sqrt{3}, \quad \sigma_6(u) = -\frac{9+5\sqrt{3}}{\sqrt{6}}u;$$
$$\sigma_7(\sqrt{2}) = -\sqrt{2}, \quad \sigma_7(\sqrt{3}) = -\sqrt{3}, \quad \sigma_7(u) = \frac{(2+\sqrt{2})(9+5\sqrt{3})}{2\sqrt{3}}u;$$
$$\sigma_8(\sqrt{2}) = -\sqrt{2}, \quad \sigma_8(\sqrt{3}) = -\sqrt{3}, \quad \sigma_8(u) = -\frac{(2+\sqrt{2})(9+5\sqrt{3})}{2\sqrt{3}}u.$$

则 $\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_8\}$. 注意到 σ_2 的阶为 2, σ_3 的阶为 4, σ_4 的阶为 4, σ_5 的阶为 4. 因此 $\mathrm{Gal}(E/\mathbb{Q}) \cong Q_8$ (四元数群). ■

4.1.5. 设 $E = \mathbb{C}(t)$ (复数域上有理函数域), $\sigma, \tau \in \mathrm{Gal}(E/\mathbb{C})$, 其中 $\sigma(t) = \omega t$, $\omega = \mathrm{e}^{2\pi \mathrm{i}/3}$, $\tau(t) = t^{-1}$. 求证:

(1) τ 和 σ 生成的群 H 是 $\mathrm{Gal}(E/\mathbb{C})$ 的 6 阶子群.

(2) $\mathrm{Inv}(H) = \mathbb{C}(t^3 + t^{-3})$.

证 令 $\alpha = t^3 + \dfrac{1}{t^3}$, $F = \mathbb{C}(\alpha)$. 令 $f(x) = x^6 - \alpha x^3 + 1 \in F[x]$, 则 $f(x)$ 的 6 个根为 $t, \omega t, \omega^2 t, \dfrac{1}{t}, \omega\dfrac{1}{t}, \omega^2\dfrac{1}{t^2}$. 于是 $f(x)$ 在 F 上的分裂域为

$$F\left(t, \omega t, \omega^2 t, \frac{1}{t}, \omega\frac{1}{t}, \omega^2\frac{1}{t^2}\right) = F\left(t, \frac{1}{t}\right) = F(t) = E.$$

因此 E/F 是有限 Galois 扩域且 $|\mathrm{Gal}(E/F)| = [E : F] = [F(t) : F] \leqslant 6$. 但另一方面, $\sigma, \tau \in \mathrm{Gal}(E/F)$, 故 $\langle \tau, \sigma \rangle \subseteq \mathrm{Gal}(E/F)$. 注意到 $\sigma^3 = 1 = \tau^2, \tau\sigma = \sigma^2\tau$ 且 $\langle \tau, \sigma \rangle$ 有 6 个元, 故 $\langle \tau, \sigma \rangle = D_3 = S_3$. 于是 $\mathrm{Gal}(E/F) = \langle \tau, \sigma \rangle$. 于是由 Galois 理论基本定理知

$$\mathrm{Inv}(\langle \tau, \sigma \rangle) = \mathrm{Inv}(\mathrm{Gal}(E/F)) = F = \mathbb{C}(t^3 + t^{-3}).$$ ■

4.1.6. 设域 F 的特征为素数 p, $\sigma \in G = \mathrm{Gal}(F(x)/F)$, 其中 $\sigma(x) = x + 1$. 令 H 为由 σ 生成的 G 之子群, 求证 $|H| = p$. 试问: $\mathrm{Inv}(H) = ?$

证 注意到 $\sigma^p = \mathrm{id}$, 因此 $H = \langle\sigma\rangle = \{1, \sigma, \cdots, \sigma^{p-1}\}$ 为 p 阶循环群. 令 $\alpha = x^p - x - 1 \in F(x)$, $K = F(\alpha)$, $E = F(x)$, 则 x 是多项式 $f(t) = t^p - t - 1 - \alpha \in K[t]$ 的根. 注意到 $f(t)$ 的全部根为 x, $x+1$, $\cdots$, $x+p-1$, 因此 $f(t)$ 在 K 上的分裂域为 $K(x) = E$. 从而 E 是 K 的有限 Galois 扩域, $|\mathrm{Gal}(E/K)| = [E:K] \leqslant p$. 另一方面 $H \subseteq \mathrm{Gal}(E/K)$. 因此 $H = \mathrm{Gal}(E/K)$. 由 Galois 理论基本定理知

$$\mathrm{Inv}(H) = \mathrm{Inv}(\mathrm{Gal}(E/K)) = K = F(x^p - x - 1). \qquad \blacksquare$$

4.1.7. 设域 F 的特征为素数 p, $a \in F$. 求证:

(1) $x^p - x - a$ 是 $F[x]$ 中不可约多项式 $\Longleftrightarrow$ 不存在 $c \in F$, 使得 $a = c^p - c$.

(2) 如果 $x^p - x - a$ 在 $F[x]$ 中不可约, 令 α 为 $x^p - x - a$ 的一个根, 求证 $F(\alpha)/F$ 为 Galois 扩张. 试决定 Galois 群 $\mathrm{Gal}(F(\alpha)/F)$.

证 (1) 设 c 是 $f(x) = x^p - x - a$ 在其分裂域中的一个根, 那么 $c, c+1, \cdots, c+p-1$ 是 $f(x)$ 的全部根. 故 $f(x)$ 为可约多项式当且仅当 $x-c$, $x-(c+1)$, $\cdots$, $x-(c+p-1)$ 这 p 个一次多项式中有 s 个乘积属于 $F(x)$, 其中 $s < p$. 由此推出这 s 个乘积的次高项系数属于 F, 从而 $c \in F$, 即存在 $c \in F$ 使得 $c^p - c = a$. 反之, 若存在 $c \in F$ 使得 $a = c^p - c$, 则 c, $c+1$, $\cdots$, $c+p-1$ 是 $f(x)$ 的全部根. 它们均在 F 中, 从而 $f(x)$ 在 $F[x]$ 中完全可裂.

(2) 此时 $f(x)$ 在 F 上的分裂域为 $F(\alpha, \alpha+1, \cdots, \alpha+p-1) = F(\alpha)$, 于是 $F(\alpha)/F$ 是有限 Galois 扩张且 $|\mathrm{Gal}(F(\alpha)/F)| = [F(\alpha):F] = p$. 故 $\mathrm{Gal}(F(\alpha)/F)$ 是 p 阶循环群, 事实上, $\mathrm{Gal}(F(\alpha)/F) = \langle\sigma\rangle$, 其中 $\sigma(\alpha) = \alpha + 1$. $\blacksquare$

4.1.8*. 设 L 和 M 均是域 E 的子域. 求证: 如果 $L/(L\bigcap M)$ 为有限 Galois 扩张, 则 LM/M 也为有限 Galois 扩张, 并且 $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/(L\bigcap M))$.

证 设 $L/(L\bigcap M)$ 是有限 Galois 扩张. 则 L 是 $L\bigcap M$ 上某个可分多项式 $f(x)$ 在 $L\bigcap M$ 上的分裂域, 即 $L = (L\bigcap M)(x_1, \cdots, x_n)$, 其中 $x_1, \cdots, x_n$ 是 $f(x)$ 的全部根. 于是 $M(x_1, \cdots, x_n) = M(L\bigcap M)(x_1, \cdots, x_n) = ML = LM$, 即 LM 是 $M[x]$ 中可分多项式 $f(x)$ 在 M 上的分裂域. 故 LM/M 是有限 Galois 扩张.

对于任一 $\sigma \in \mathrm{Gal}(LM/M)$, σ 是 $x_1, \cdots, x_n$ 的一个置换, 故 $\sigma(L) = L$, 于是 $\sigma \in \mathrm{Gal}(L/L\bigcap M)$. 这就给出 $\mathrm{Gal}(LM/M)$ 到 $\mathrm{Gal}(L/L\bigcap M)$ 的群同态, 易知这个同态的核是 $\{1\}$.

剩下只要证明 $[LM:M] = [L:L\bigcap M]$. 因 $L/L\bigcap M$ 是有限可分扩张, 故 $L = (L\bigcap M)(\alpha)$. 设 $g(x)$ 是 α 在 $L\bigcap M$ 上的极小多项式. 因 $LM = M(\alpha)$, 故只要证 $g(x)$ 也是 α 在 M 上的极小多项式, 即要证 $g(x)$ 在 $M[x]$ 中不可约.

设 $g(x)$ 在 $M[x]$ 中有分解 $g(x) = h(x)l(x)$. 因 $L/L\bigcap M$ 正规, 故 L 包含 $g(x)$ 的全部根 $\alpha_1 = \alpha, \cdots, \alpha_m$. 注意到 $h(x)$ 和 $l(x)$ 的系数均是这些根的系数为

± 1 的多项式, 从而 $h(x)$ 和 $l(x)$ 的系数属于 $L\bigcap M$. 所以, 由 $g(x)$ 在 $L\bigcap M$ 上的不可约性即知 $g(x)$ 在 $M[x]$ 中的不可约性. 这就完成了证明. ■

4.1.9. 设 E/F 为有限 Galois 扩张, N 和 M 为中间域, $E\supseteq N\supseteq M\supseteq F$, 并且 N 是 M 在 F 上的正规闭包. 求证:

$$\mathrm{Gal}(E/N)=\bigcap_{\sigma\in\mathrm{Gal}(E/F)}\sigma\mathrm{Gal}(E/M)\sigma^{-1}.$$

证 根据 Galois 理论基本定理, 只要证

$$\mathrm{Inv}(\mathrm{Gal}(E/N))=\mathrm{Inv}\left(\bigcap_{\sigma\in\mathrm{Gal}(E/F)}\sigma\mathrm{Gal}(E/M)\sigma^{-1}\right),$$

即只要证

$$N=\prod_{\sigma\in\mathrm{Gal}(E/F)}\mathrm{Inv}(\sigma\mathrm{Gal}(E/M)\sigma^{-1}),$$

即只要证

$$N=\prod_{\sigma\in\mathrm{Gal}(E/F)}\sigma(M).\tag{$*$}$$

下证 $(*)$ 式成立. 因为 $\bigcap\limits_{\sigma\in\mathrm{Gal}(E/F)}\sigma\mathrm{Gal}(E/M)\sigma^{-1}$ 是 $\mathrm{Gal}(E/F)$ 的正规子群, 故 $\prod\limits_{\sigma\in\mathrm{Gal}(E/F)}\sigma(M)$ 是 F 的正规扩域且包含 M. 而 N 是包含 M 的 F 的最小正规扩域, 因此有

$$N\subseteq\prod_{\sigma\in\mathrm{Gal}(E/F)}\sigma(M).$$

另一方面, 由定义

$$N:=\bigcap_{\substack{M\subseteq T\subseteq\Omega,\\ T/F\text{正规}}}T,$$

其中 Ω 为 M 的代数闭包. 我们断言

$$N=\bigcap_{\substack{M\subseteq K\subseteq E,\\ K/F\text{正规}}}K.$$

事实上

$$\bigcap_{\substack{M\subseteq K\subseteq E,\\ K/F\text{正规}}}K\supseteq N.$$

反之, 对于任一 T, 其中 $M \subseteq T \subseteq \Omega$, T/F 正规, $(T \bigcap E)/F$ 也正规. 因此

$$N = \bigcap_{\substack{M \subseteq K \subseteq E, \\ K/F\text{正规}}} K.$$

对于任一 $\sigma \in \mathrm{Gal}(E/F)$, 且对于任一 K, 其中 $M \subseteq K \subseteq E$, K/F 正规, 由于 $M \subseteq K$, 故 $\sigma(M) \subseteq \sigma(K)$. 而 K/F 正规, 因此 $\sigma(K) = K$. 这表明 $\sigma(M) \subseteq K$, 从而

$$\prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(M) \subseteq \bigcap_{\substack{M \subseteq K \subseteq E, \\ K/F\text{正规}}} K = N.$$

这就证明了 $(*)$ 式成立. ■

4.1.10. 设 E 为 $x^4 - 2$ 在 $\mathbb{Q}$ 上的分裂域.

(1) 试求出 $E/\mathbb{Q}$ 的全部中间域.

(2) 试问哪些中间域是 $\mathbb{Q}$ 的 Galois 扩张? 哪些域彼此共轭?

解 (1) 因为

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}\mathrm{i})(x + \sqrt[4]{2}\mathrm{i}),$$

故 $E = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}\mathrm{i}, -\sqrt[4]{2}\mathrm{i}) = \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$, $[E:\mathbb{Q}] = 8$, $|\mathrm{Gal}(E/\mathbb{Q})| = 8$, $\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_1 = \mathrm{id}, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8\}$, 其中

$$\begin{aligned}
&\sigma_2(\mathrm{i}) = \mathrm{i}, \quad \sigma_2(\sqrt[4]{2}) = -\sqrt[4]{2}; && \sigma_3(\mathrm{i}) = \mathrm{i}, \quad \sigma_3(\sqrt[4]{2}) = \sqrt[4]{2}\mathrm{i};\\
&\sigma_4(\mathrm{i}) = \mathrm{i}, \quad \sigma_4(\sqrt[4]{2}) = -\sqrt[4]{2}\mathrm{i}; && \sigma_5(\mathrm{i}) = -\mathrm{i}, \quad \sigma_5(\sqrt[4]{2}) = \sqrt[4]{2};\\
&\sigma_6(\mathrm{i}) = -\mathrm{i}, \quad \sigma_6(\sqrt[4]{2}) = -\sqrt[4]{2}; && \sigma_7(\mathrm{i}) = -\mathrm{i}, \quad \sigma_7(\sqrt[4]{2}) = \sqrt[4]{2}\mathrm{i};\\
&\sigma_8(\mathrm{i}) = -\mathrm{i}, \quad \sigma_8(\sqrt[4]{2}) = -\sqrt[4]{2}\mathrm{i}.
\end{aligned}$$

易知 $\mathrm{Gal}(E/\mathbb{Q}) \cong D_4$, 其全部非平凡子群为

$$\{1, \sigma_2\}, \quad \{1, \sigma_5\}, \quad \{1, \sigma_6\}, \quad \{1, \sigma_7\}, \quad \{1, \sigma_8\},$$

$$\{1, \sigma_3,\ \sigma_2,\ \sigma_4\} = \langle \sigma_3 \rangle = \langle \sigma_4 \rangle, \quad \{1, \sigma_2,\ \sigma_5, \sigma_6\}, \quad \{1, \sigma_2,\ \sigma_7,\ \sigma_8\}.$$

它们对应着 $E/\mathbb{Q}$ 的全部中间域, 依次为

$$\mathbb{Q}(\mathrm{i}, \sqrt{2}), \quad \mathbb{Q}(\sqrt[4]{2}), \quad \mathbb{Q}(\sqrt[4]{2}\mathrm{i}), \quad \mathbb{Q}(\sqrt[4]{2}(1+\mathrm{i})), \quad \mathbb{Q}(\sqrt[4]{2}(1-\mathrm{i})),$$

$$\mathbb{Q}(\mathrm{i}), \quad \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{2}\mathrm{i}).$$

(2) 这八个中间域中, $\mathbb{Q}(\mathrm{i},\sqrt{2})$, $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}\mathrm{i})$ 是 $\mathbb{Q}$ 的 Galois 扩张. $\mathbb{Q}(\sqrt[4]{2})$ 与 $\mathbb{Q}(\sqrt[4]{2}\mathrm{i})$ 共轭, $\mathbb{Q}(\sqrt[4]{2}(1+\mathrm{i}))$ 与 $\mathbb{Q}(\sqrt[4]{2}(1-\mathrm{i}))$ 共轭. 除此之外没有其他共轭的域, 这可从群方面来看. ■

4.1.11. 设 $\zeta=\mathrm{e}^{\frac{2\pi\mathrm{i}}{12}}$, 求证 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 是 Galois 扩张. 求 $G=\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. 列出 G 的全部子群和它们对应的 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 的中间域.

解 $\zeta=\mathrm{e}^{\frac{2\pi\mathrm{i}}{12}}$ 是 12 次本原单位根.

$$\begin{aligned}x^{12}-1&=(x^6-1)(x^6+1)\\&=(x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)(x^4-x^2+1).\end{aligned}$$

ζ 在 $\mathbb{Q}$ 上的极小多项式为 x^4-x^2+1, $\mathbb{Q}(\zeta)$ 是 $x^{12}-1$ 在 $\mathbb{Q}$ 上的分裂域. 因此 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 是 Galois 扩张且 $[\mathbb{Q}(\zeta):\mathbb{Q}]=4$, $G=\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 是 Klein 四元群. 事实上, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})=\{\sigma_1=\mathrm{id},\sigma_2=\tau,\sigma_3=\eta,\sigma_4=\tau\eta\}$, 其中 $\tau(\zeta)=\zeta^5$, $\eta(\zeta)=\zeta^7$.

由此可知 G 的全部子群为 $\{1\}$, $\langle\tau\rangle$, $\langle\eta\rangle$, $\langle\tau\eta\rangle$, G. 它们所对应的 $\mathbb{Q}(\xi)/\mathbb{Q}$ 的中间域依次为 $\mathbb{Q}(\zeta)$, $\mathbb{Q}(\zeta^2)=\mathbb{Q}(\zeta^4)=\mathbb{Q}(\zeta^8)=\mathbb{Q}(\zeta^{10})$, $\mathbb{Q}(\zeta^3)=\mathbb{Q}(\zeta^9)$, $\mathbb{Q}(\zeta^8+\zeta^4)$, $\mathbb{Q}$. ■

4.1.12. 对 $\zeta=\mathrm{e}^{\frac{2\pi}{9}\mathrm{i}}$ 做题 4.1.11 的事情.

解 $\zeta=\mathrm{e}^{\frac{2\pi}{9}\mathrm{i}}$ 是 9 次本原单位根.

$$x^9-1=(x^3-1)(x^6+x^3+1)=(x-1)(x^2+x+1)(x^6+x^3+1).$$

ζ 在 $\mathbb{Q}$ 上的极小多项式为 x^6+x^3+1, $\mathbb{Q}(\zeta)$ 是 x^6+x^3+1 在 $\mathbb{Q}$ 上的分裂域. 因此 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 是 Galois 扩张且 $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|=6$.

令 $\sigma_i(\zeta)=\zeta^i$, $i=1, 2, 4, 5, 7, 8$. 则 $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})=\{\sigma_1,\sigma_2,\sigma_4,\sigma_5,\sigma_7,\sigma_8\}=\langle\sigma_2\rangle$ 是 6 阶循环群.

因此 $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 的非平凡子群为 2 阶子群 $\langle\sigma_2^3\rangle=\langle\sigma_8\rangle$ 和 3 阶子群 $\langle\sigma_2^2\rangle=\langle\sigma_4\rangle$. 它们所对应的 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 的中间域分别为三次扩域 $\mathbb{Q}(\zeta^3+\zeta^6)$ 和二次扩域 $\mathbb{Q}(\zeta^3)=\mathbb{Q}(\zeta^6)$. ■

4.1.13. 设 n 为大于 2 的整数, $\zeta_n=\mathrm{e}^{\frac{2\pi}{n}\mathrm{i}}$, $\mathbb{R}$ 为实数域. 求证: $\mathbb{Q}(\zeta_n)\bigcap\mathbb{R}=\mathbb{Q}(\zeta_n+\zeta_n^{-1})$.

证 由于 $\zeta_n+\zeta_n^{-1}=\mathrm{e}^{\frac{2\pi}{n}\mathrm{i}}+\mathrm{e}^{-\frac{2\pi}{n}\mathrm{i}}=2\cos\dfrac{2\pi}{n}\in\mathbb{R}$, 因此 $\mathbb{Q}(\zeta_n+\zeta_n^{-1})\subseteq\mathbb{R}\bigcap\mathbb{Q}(\zeta_n)$.

反之, 先设 $n=2m+1$, $m\geqslant 1$. 对于任一 $x=\sum\limits_{t=1}^{n-1}a_t\zeta_n^t\in\mathbb{R}\bigcap\mathbb{Q}(\zeta_n)$, x 的虚

部为 0, 即 $\sum_{t=1}^{n-1} a_t \sin\frac{2\pi t}{n}=0$. 而

$$\sum_{t=1}^{n-1} a_t \sin\frac{2\pi t}{n}=\sum_{t=1}^{m}(a_t-a_{n-t})\sin\frac{2\pi t}{n}.$$

由 Fourier 分析知, $\sin\frac{2\pi}{n}$, $\sin\frac{4\pi}{n}$, $\cdots$, $\sin\frac{2m\pi}{n}$ 是 $\mathbb{Q}$- 线性无关的, 因此 $a_n - a_{n-t}=0$. 于是

$$x=\sum_{t=1}^{n-1} a_t\zeta_n^t=\sum_{t=1}^{m}(a_t\zeta_n^t+a_{n-t}\zeta_n^{n-t})=\sum_{t=1}^{m}a_t(\zeta_n^t+\zeta_n^{-t})\in\mathbb{Q}(\zeta_n+\zeta_n^{-1}).$$

其中最后一步由二项式系数的性质和归纳法可推知.

对于 $n=2m$, $m\geqslant 1$, 类似地讨论. ■

4.1.14*. 设 p 为奇素数, $\zeta_p=\mathrm{e}^{\frac{2\pi}{p}\mathrm{i}}$. 求证 $\mathbb{Q}(\zeta_p)$ 有唯一的二次子域 K (即 K 为 $\mathbb{Q}(\zeta_p)$ 的子域并且 $[K:\mathbb{Q}]=2$). 进而, K 是实二次域 (即 $K\subseteq\mathbb{R}$) $\Longleftrightarrow$ $p\equiv 1 \pmod 4$.

注 在解本题之前, 回忆若干预备知识. 用 $\mathbb{Z}_n$ 表示模 n 的剩余类加法群, 用 $\mathbb{Z}_n^*$ 表示 $\mathbb{Z}_n$ 中的剩余类 $\bar{s}$, $1\leqslant s\leqslant n-1$, $(s,n)=1$ 作成的 $\varphi(n)$ 阶 Abel 群, 其中 $\varphi(n)$ 是 Euler 函数. 对于整数 $n>1$, 整数 g 称为模 n 的原根, 如果 $(g,n)=1$ 且 $\bar{g}$ 在 $\mathbb{Z}_n^*$ 中的乘法阶为 $\varphi(n)$. 因此模 n 的原根存在当且仅当 $\mathbb{Z}_n^*$ 是循环群, 此时 $\mathbb{Z}_n^*$ 的任一生成元 $\bar{g}$ 就给出模 n 的一个原根 g. 对哪些 $n>1$, 存在模 n 的原根, 是一个有趣的问题. 例如, 可参阅 [FY]. 对于任一素数 p, $\mathbb{Z}_p$ 成为域, 故 $\mathbb{Z}_p^*$ 恰是域 $\mathbb{Z}_p$ 的乘法群, 因此是循环群. 即模 p 的原根总存在.

证 因 ζ_p 是 p 次本原单位根, 故 $\mathbb{Q}(\zeta_p)$ 是 x^p-1 在 $\mathbb{Q}$ 上的分裂域, 从而 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 是有限 Galois 扩张. 因 ζ_p 在 $\mathbb{Q}$ 上的极小多项式为 $x^{p-1}+x^{p-2}+\cdots+x+1$, 故 $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$. 故 G 是 $p-1$ 阶群, 其中 $G=\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. 令 g 是模 p 的一个原根, 并令 $\sigma:\ \zeta_p\longmapsto\zeta_p^g$, 则 $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, 且 σ 的阶为 $p-1$, 即 $G=\langle\sigma\rangle$. 因为 G 有唯一的 $\frac{p-1}{2}$ 阶子群 $H=\langle\sigma^2\rangle$, 故由 Galois 理论基本定理知 $\mathbb{Q}(\zeta_p)$ 有唯一的二次子域 K, 且 $K=\mathrm{Inv}(\langle\sigma^2\rangle)$, 其中 $\sigma^2(\zeta_p^t)=\zeta_p^{g^2t}$, $t=1,\cdots,p-1$.

K 为实二次域当且仅当 $K\subseteq\mathbb{R}\bigcap\mathbb{Q}(\zeta_p)=\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ (由题 4.1.13 的结论). 注意到

$$\mathbb{Q}(\zeta_p+\zeta_p^{-1})=\left\{\sum_{t=1}^{p-1}a_t\zeta_p^t\ \middle|\ a_1=a_{p-1},\ a_2=a_{p-2},\cdots,\ a_{\frac{p-1}{2}}=a_{\frac{p+1}{2}}\right\}.$$

另一方面

$$K=\mathrm{Inv}(\langle\sigma^2\rangle)=\left\{x=\sum_{t=1}^{p-1}a_t\zeta_p^t\ \middle|\ \sigma^2(x)=x\right\}$$
$$=\left\{\sum_{t=1}^{p-1}a_t\zeta_p^t\ \middle|\ \sum_{t=1}^{p-1}a_t\zeta_p^{g^2t}=\sum_{t=1}^{p-1}a_t\zeta_p^t\right\}.$$

因此 K 为实二次域当且仅当

$$\left\{\sum_{t=1}^{p-1}a_t\zeta_p^t\ \middle|\ \sum_{t=1}^{p-1}a_t\zeta_p^{g^2t}=\sum_{t=1}^{p-1}a_t\zeta_p^t\right\}\subseteq\mathbb{Q}(\zeta_p+\zeta_p^{-1}),$$

当且仅当由 $\sum_{t=1}^{p-1}a_t\zeta_p^{g^2t}=\sum_{t=1}^{p-1}a_t\zeta_p^t$ 可推出

$$a_1=a_{p-1},\ a_2=a_{p-2},\cdots,\ a_{\frac{p-1}{2}}=a_{\frac{p+1}{2}}.$$

由 $\sum_{t=1}^{p-1}a_t\zeta_p^{g^2t}=\sum_{t=1}^{p-1}a_t\zeta_p^t$, 比较两边 $\zeta_p^{g^2}$ 的系数知 $a_1=a_{g^2}$ (注意下标是模 p 的). 再比较两边 $\zeta_p^{g^4}$ 的系数知 $a_{g^2}=a_{g^4}$. 继续下去即得

$$a_1=a_{g^2}=a_{g^4}=a_{g^6}=\cdots=a_{g^{2s}}.$$

因此, 若 K 为实二次域, 取 $\zeta_p+\zeta_p^{g^2}+\zeta_p^{g^4}+\zeta_p^{g^6}+\cdots\in K$ 即可看出存在 s 使得 $g^{2s}\equiv-1\pmod p$. 而 -1 模 p 的乘法阶为 2, 故 g^{2s} 模 p 的乘法阶为 2, 即 $\frac{p-1}{(2s,p-1)}=2$, $(2s,p-1)=\frac{p-1}{2}$. 由此即知 $\frac{p-1}{2}$ 是偶数, 即 $p\equiv1(\mathrm{mod}\ 4)$.

反之, 若 $p=4s+1$, 则 g^{2s} 模 p 的乘法阶为 2. 因此 $g^{2s}\equiv-1\pmod p$. 因此由上所述, 由 $\sum_{t=1}^{p-1}a_t\zeta_p^{g^2t}=\sum_{t=1}^{p-1}a_t\zeta_p^t$ 可推出

$$a_1=a_{g^2}=\cdots=a_{g^{2s}}=a_{-1}.$$

对于任一 t, $1\leqslant t\leqslant\frac{p-1}{2}$, 由 $\sum_{j=1}^{p-1}a_j\zeta_p^{g^2j}=\sum_{j=1}^{p-1}a_j\zeta_p^j$ 可推出

$$a_t=a_{g^2t}=a_{g^4t}=\cdots=a_{g^{2s}t}=a_{-t}.$$

从而 K 为实二次域. ■

4.1.15. 设 E/F 为有限 Galois 扩张. 如果对任一域 K $(F\subsetneqq K\subseteq E)$, K 对 F 均有相同的扩张次数 $[K:F]$, 则 $[E:F]=p$, p 为素数.

证 令 $G = \mathrm{Gal}(E/F)$. 由 Galois 理论基本定理可知此题目可以翻译成: 若 G 的任一真子群 H 均有相同的指数, 则 $|G| = p$. 即若 G 的任一真子群均有相同的阶, 则 G 为 p 阶循环群. 而由 Sylow 定理这是显然的. ■

4.1.16. (1) 求证 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}$ 是 Galois 扩张, 并求此扩张的 Galois 群.

(2) 求元 $\sqrt{6}+\sqrt{10}+\sqrt{15}$ 在 $\mathbb{Q}$ 上的极小多项式.

(3) 求证 $\sqrt{6} \in \mathbb{Q}\,(\sqrt{6}+\sqrt{10}+\sqrt{15})$.

(4) 求 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}\,(\sqrt{6}+\sqrt{10}+\sqrt{15})$ 上的极小多项式.

解 (1) $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ 是 $f(x) = (x^2-2)(x^2-3)(x^2-5) \in \mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上的分裂域, 因此是 Galois 扩张. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ 是 8 阶群. 令

$$
\begin{array}{lll}
\sigma_1 = \mathrm{id}; & & \\
\sigma_2(\sqrt{2}) = \sqrt{2}, & \sigma_2(\sqrt{3}) = \sqrt{3}, & \sigma_2(\sqrt{5}) = -\sqrt{5}; \\
\sigma_3(\sqrt{2}) = \sqrt{2}, & \sigma_3(\sqrt{3}) = -\sqrt{3}, & \sigma_3(\sqrt{5}) = \sqrt{5}; \\
\sigma_4(\sqrt{2}) = \sqrt{2}, & \sigma_4(\sqrt{3}) = -\sqrt{3}, & \sigma_4(\sqrt{5}) = -\sqrt{5}; \\
\sigma_5(\sqrt{2}) = -\sqrt{2}, & \sigma_5(\sqrt{3}) = \sqrt{3}, & \sigma_5(\sqrt{5}) = \sqrt{5}; \\
\sigma_6(\sqrt{2}) = -\sqrt{2}, & \sigma_6(\sqrt{3}) = \sqrt{3}, & \sigma_6(\sqrt{5}) = -\sqrt{5}; \\
\sigma_7(\sqrt{2}) = -\sqrt{2}, & \sigma_7(\sqrt{3}) = -\sqrt{3}, & \sigma_7(\sqrt{5}) = \sqrt{5}; \\
\sigma_8(\sqrt{2}) = -\sqrt{2}, & \sigma_8(\sqrt{3}) = -\sqrt{3}, & \sigma_8(\sqrt{5}) = -\sqrt{5}.
\end{array}
$$

故 $\mathrm{Gal}(\mathbb{Q}\,(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})=\{\sigma_1,\cdots,\sigma_8\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

(2) 设 $f(x)$ 是 $\alpha = \sqrt{6}+\sqrt{10}+\sqrt{15}$ 在 $\mathbb{Q}$ 上的极小多项式. 考虑集合 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})(\alpha) = \{\alpha,\ \beta = \sqrt{6}-\sqrt{10}-\sqrt{15},\ \gamma = -\sqrt{6}+\sqrt{10}-\sqrt{15},\ \delta = -\sqrt{6}-\sqrt{10}+\sqrt{15}\}$. 取 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ 使得 $\sigma(\alpha) = \beta$. 在 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ 中, $0 = f(\alpha)$. 两边作用 σ 得到 $0 = f(\beta)$. 同理可得到 γ, δ 均是 $f(x)$ 的根. 另一方面,

$$
\begin{aligned}
&(x-\alpha)(x-\beta)(x-\gamma)(x-\delta) \\
=& (x^2-(\alpha+\beta)x+\alpha\beta)(x^2-(\gamma+\delta)x+\gamma\delta) \\
=& (x^2-2\sqrt{6}x-10\sqrt{6}-19)(x^2+2\sqrt{6}x+10\sqrt{6}-19) \\
=& (x^2-19)^2-(2\sqrt{6}x+10\sqrt{6})^2 \\
=& (x^4-38x^2+361)-24(x+5)^2 \\
=& x^4-62x^2-240x-239 \in \mathbb{Q}(x).
\end{aligned}
$$

通过计算可知 $(x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$ 的任一正次数的真因子不再属于 $\mathbb{Q}[x]$. 从而 $x^4-62x^2-240x-239$ 就是 $\sqrt{6}+\sqrt{10}+\sqrt{15}$ 在 $\mathbb{Q}$ 上的极小多项式.

(3) 令 $\alpha = \sqrt{6}+\sqrt{10}+\sqrt{15}$. 则 $\alpha^2 = 4\alpha+31+2\sqrt{10}+6\sqrt{6}$, $\alpha^3 = 4\alpha^2+41\alpha+56+8\sqrt{10}+6\sqrt{15}$. 因此

$$\begin{pmatrix} 1 & 1 & 1 \\ 6 & 2 & 0 \\ 0 & 8 & 6 \end{pmatrix} \begin{pmatrix} \sqrt{6} \\ \sqrt{10} \\ \sqrt{15} \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha^2-4\alpha-31 \\ \alpha^3-4\alpha^2-41\alpha-56 \end{pmatrix}.$$

因 $\begin{pmatrix} 1 & 1 & 1 \\ 6 & 2 & 0 \\ 0 & 8 & 6 \end{pmatrix}$ 是可逆阵, 故 $\sqrt{6}, \sqrt{10}, \sqrt{15} \in \mathbb{Q}(\alpha)$.

(4) 令 $\alpha = \sqrt{6}+\sqrt{10}+\sqrt{15}$. 因 $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$, 故 $\beta = \sqrt{2}+\sqrt{3}$ 满足 $\mathbb{Q}(\alpha)[x]$ 中多项式 $x^2-5-2\sqrt{6}$. 因 $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4 = [\mathbb{Q}(\alpha):\mathbb{Q}]$, 若 $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\alpha)$, 则 $\sqrt{5} = \dfrac{\alpha-\sqrt{6}}{\sqrt{2}+\sqrt{3}} \in \mathbb{Q}(\alpha)$, 进而由本题 (3) 知 $\sqrt{2}$, $\sqrt{3} \in \mathbb{Q}(\alpha)$. 于是 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) = \mathbb{Q}(\alpha)$. 但 $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}] = 8 \neq 4 = [\mathbb{Q}(\alpha):\mathbb{Q}]$. 矛盾! 于是 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\alpha)$ 上的极小多项式为 $x^2-5-2\sqrt{6}$. ■

§2 方程的 Galois 群

知识要点:

设 E 是 n $(n \geqslant 1)$ 次多项式 $f(x)$ 在 F 上的分裂域. 将 Galois 群 $\mathrm{Gal}(E/F)$ 称为多项式 $f(x)$ 或方程 $f(x) = 0$ 在 F 上的 Galois 群, 记为 $\mathrm{Gal}(f(x), F)$, 或 G_f.

G_f 是 $f(x)$ 的根集的一个置换群; 若 $f(x)$ 在 F 上可分, 则 $|\mathrm{Gal}(f(x),F)| = [E:F]$.

设 $f(x)$ 无重根, 则 G_f 是对称群 S_n 的可迁子群当且仅当 $f(x)$ 在 $F[x]$ 中不可约.

设 $r_1, \cdots, r_n$ 是无重根多项式 $f(x)$ 的全部根, 令 $D = \prod\limits_{1\leqslant i<j\leqslant n}(r_i-r_j)$, 称 $d(f) = D^2 \in F$ 为 $f(x)$ 在 F 上的判别式. 若 $\mathrm{Char}\, F \neq 2$, 则 $\mathrm{Gal}(E/F(D)) = \mathrm{G}_f \bigcap A_n$; 从而 $\mathrm{G}_f \subseteq A_n$ 当且仅当 $D \in F$. 故当 $\mathrm{Char}\, F \neq 2$ 时, 对于三次 (无重根) 不可约多项式 $f(x)$ 有

$$\mathrm{Gal}(f(x), F) = \begin{cases} A_3, & D \in F, \\ S_3, & D \notin F. \end{cases}$$

若素数 p 次不可约多项式 $f(x) \in \mathbb{Q}[x]$ 只有两个非实的复根, 则 $\mathrm{Gal}(f(x), \mathbb{Q}) = S_p$.

n 次一般方程 $f(x)=x^n+t_1x^{n-1}+\cdots+t_{n-1}x+t_n=0$ 在域 $F(t_1,\cdots,t_n)$ 上的 Galois 群为 S_n, 这里 $t_1,\cdots,t_n$ 是域 F 上的独立的代数无关元.

4.2.1. 设 F 是特征为 2 的域. 求 $f(x)$ 在 F 上的 Galois 群, 其中

(1) $f(x)=x^3+x+1$.

(2) $f(x)=x^3+x^2+1$.

解 (1) 设 r 是 $f(x)$ 的一个根, 容易验证 r, r^2, r^2+r 是 $f(x)$ 的 (两两不同的) 根. 当 $r\notin F$ 时, 容易验证 $f(x)$ 在 F 上不可约, 从而 $|\mathrm{G}_f|=|\mathrm{Gal}(F(r)/F)|=[F(r):F]=3$. 而 S_3 的 3 阶子群是 A_3. 故

$$\mathrm{G}_f=\mathrm{Gal}(F(r)/F)=\begin{cases}\{1\}, & r\in F,\\ A_3, & r\notin F.\end{cases}$$

(2) 设 r 是 $f(x)$ 的一个根, 则易验证 r, r^2, r^2+r+1 是 $f(x)$ 的 (两两不同的) 根. 同理可知

$$\mathrm{G}_f=\mathrm{Gal}(F(r)/F)=\begin{cases}\{1\}, & r\in F,\\ A_3, & r\notin F.\end{cases}$$ ■

4.2.2. 设 $f(x)\in\mathbb{R}[x]$ 是三次不可约多项式. 求证: $d(f)>0$ 当且仅当 $f(x)$ 有三个实根; $d(f)<0$ 当且仅当 $f(x)$ 只有一个实根.

证 实系数不可约多项式无重根. 奇数次实系数多项式总有实根 (因为非实的复根是共轭成对出现的). 故三次实系数多项式或者有三个实根, 或者只有一个实根.

若 $d(f)>0$, 则 $f(x)$ 必有三个实根. 否则 $f(x)$ 的三个根具有形式 $r_1\in\mathbb{R}$, $r_2=a+b\mathrm{i}$, $r_3=a-b\mathrm{i}$, $a,\ b\in\mathbb{R}$, $b\neq0$, 其中 $\mathrm{i}=\sqrt{-1}$. 于是

$d(f)=(r_1-r_2)^2(r_1-r_3)^2(r_2-r_3)^2=-4b^2((r_1-a)^2+b^2)^2<0$.

若 $d(f)<0$, 则 $f(x)$ 只有一个实根. 否则由 $d(f)$ 的定义知 $d(f)>0$. ■

4.2.3. 求 Galois 群 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}(1+\mathrm{i}))/\mathbb{Q})$, 其中 $\mathrm{i}=\sqrt{-1}$.

解 令 $\alpha=\sqrt[4]{2}(1+\mathrm{i})$, 则 α 在 $\mathbb{Q}$ 上的极小多项式为 x^4+8. 故 $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$. 这个极小多项式的全部根为 $\pm\sqrt[4]{2}(1+\mathrm{i})$, $\pm\sqrt[4]{2}(1-\mathrm{i})$. 因 $\sqrt[4]{2}(1-\mathrm{i})\notin\mathbb{Q}(\alpha)$, 从而 Galois 群 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}(1+\mathrm{i}))/\mathbb{Q})$ 中元 σ 只能将 α 变为 $\pm\alpha$. 即 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}(1+\mathrm{i}))/\mathbb{Q})$ 是 2 阶循环群. 注意 $\mathbb{Q}(\sqrt[4]{2}(1+\mathrm{i}))/\mathbb{Q}$ 不是正规扩张. ■

4.2.4. 设 p 为素数, $a\in\mathbb{Q}$, x^p-a 为 $\mathbb{Q}[x]$ 中不可约多项式. 求 x^p-a 在 $\mathbb{Q}$ 上的 Galois 群.

解 设 E 是 x^p-a 在 $\mathbb{Q}$ 上的分裂域. 不妨设 $a>0$ ($a<0$ 的情形类似讨论). 于是 $E=\mathbb{Q}(\sqrt[p]{a},\ \omega)$, 其中 ω 是 p 次本原单位根. 因 ω 在 $\mathbb{Q}$ 上的极

小多项式为 $x^{p-1}+x^{p-2}+\cdots+x+1$, $\sqrt[p]{a}$ 在 $\mathbb{Q}$ 上的极小多项式为 x^p-a, 故 $|\mathrm{Gal}(E/\mathbb{Q})|=p(p-1)$. 任取 $\sigma\in\mathrm{Gal}(E/\mathbb{Q})$, 则 $\sigma(\sqrt[p]{a})=\sqrt[p]{a}\omega^l$, $0\leqslant l\leqslant p-1$; $\sigma(\omega)=\omega^k$, $1\leqslant k\leqslant p-1$. 由于 σ 完全由它在 $\sqrt[p]{a}$ 和 ω 上的值唯一确定, 因此 σ 完全由 k 和 l 唯一确定. 记 $\sigma=\sigma_{k,l}$, 则

$$\psi:\ \mathrm{Gal}(E/\mathbb{Q})\longrightarrow GL(2,F_p);\quad \sigma_{k,l}\mapsto\begin{pmatrix}k & l\\ 0 & 1\end{pmatrix}.$$

容易验证 ψ 是群同构. 因此 x^p-a 在 $\mathbb{Q}$ 上的 Galois 群同构于 p 元域 F_p 上 2 阶一般线性群 $GL(2,F_p)$ 的子群

$$\left\{\begin{pmatrix}k & l\\ 0 & 1\end{pmatrix}\ \middle|\ l,k\in F_p,\ k\neq 0\right\}.$$ ■

4.2.5. 决定 $f(x)$ 在 $\mathbb{Q}$ 上的 Galois 群, 其中

(1) $f(x)=x^5-6x+3$.

(2) $f(x)=x^5-15x^2+9$.

解 (1) 首先由 Eisenstein 判别法知 $f(x)=x^5-6x+3$ 是 $\mathbb{Q}[x]$ 中不可约多项式. 由初等微积分易知 $f(x)$ 恰有三个实根, 从而恰有两个非实的复根 (细节略去). 因此 $\mathrm{Gal}(f(x))=S_5$.

(2) 在 $\mathbb{Z}_2[x]$ 中 $f(x)=x^5-15x^2+9=x^5+x^2+1$ 无一次因子; $\mathbb{Z}_2[x]$ 中唯一的二次不可约多项式不是 x^5+x^2+1 的因子. 因此 $f(x)$ 在 $\mathbb{Z}_2[x]$ 中, 从而在 $\mathbb{Q}$ 上不可约.

再由初等微积分易知 $f(x)$ 恰有三个实根, 从而恰有两个非实的复根 (细节略去). 因此 $\mathrm{Gal}(f(x))=S_5$. ■

4.2.6. 决定 $f(x)$ 在域 F 上的 Galois 群, 其中

(1) $f(x)=x^4-5$, $F=\mathbb{Q}$.

(2) $f(x)=x^4-5$, $F=\mathbb{Q}(\sqrt{5})$.

(3) $f(x)=x^4-5$, $F=\mathbb{Q}(\sqrt{5}\,\mathrm{i})$.

(4) $f(x)=x^4-10x^2+4$, $F=\mathbb{Q}$.

解 (1) $f(x)=x^4-5\in\mathbb{Q}[x]$ 是四次不可约多项式. 由 $f(x)$ 诱导出来的三次多项式 $g(x)$ 为 $g(x)=x^3+20x=x(x^2+20)=x(x+2\sqrt{5}\mathrm{i})(x-2\sqrt{5}\mathrm{i})$.

而 $[\mathbb{Q}(\sqrt{5}\mathrm{i}):\mathbb{Q}]=2$. 又因 $f(x)$ 在 $\mathbb{Q}(\sqrt{5}\mathrm{i})[x]$ 中不可约, 故由四次方程 Galois 群的一般结论知 $\mathrm{Gal}(f(x),\mathbb{Q})=D_4$ (二面体群).

注 也可以不用四次方程 Galois 群的一般结论而直接计算. 因 $f(x)$ 在 $\mathbb{Q}$ 上

的分裂域 $\mathbb{Q}(\sqrt[4]{5},\mathrm{i})$ 相对于 $\mathbb{Q}$ 的维数是 8, 故 $\mathrm{Gal}(f(x),\mathbb{Q})$ 是 8 阶群, 这 8 个元为

$$\tau_1=\mathrm{id};\qquad \tau_2:\ \sqrt[4]{5}\longmapsto -\sqrt[4]{5},\ \mathrm{i}\longmapsto \mathrm{i};$$

$$\tau_3:\ \sqrt[4]{5}\longmapsto \sqrt[4]{5}\mathrm{i},\ \ \mathrm{i}\longmapsto \mathrm{i};\qquad \tau_4:\ \sqrt[4]{5}\longmapsto -\sqrt[4]{5}\mathrm{i},\ \ \mathrm{i}\longmapsto \mathrm{i};$$

$$\tau_5:\ \sqrt[4]{5}\longmapsto \sqrt[4]{5},\ \ \mathrm{i}\longmapsto -\mathrm{i};\qquad \tau_6:\ \sqrt[4]{5}\longmapsto -\sqrt[4]{5},\ \ \mathrm{i}\longmapsto -\mathrm{i};$$

$$\tau_7:\ \sqrt[4]{5}\longmapsto \sqrt[4]{5}\mathrm{i},\ \ \mathrm{i}\longmapsto -\mathrm{i};\qquad \tau_8:\ \sqrt[4]{5}\longmapsto -\sqrt[4]{5}\mathrm{i},\ \ \mathrm{i}\longmapsto -\mathrm{i}.$$

易知 4 阶元 τ_3 和 2 阶元 τ_5 生成 $\mathrm{Gal}(f(x),\mathbb{Q})$ 且 $\tau_5\tau_3=\tau_3^3\tau_5$. 从而 $\mathrm{Gal}(f(x),\mathbb{Q})$ 是二面体群.

(2) $f(x)=x^4-5\in\mathbb{Q}(\sqrt{5})[x]$ 是可约多项式, 即有

$$x^4-5=(x^2-\sqrt{5})(x^2+\sqrt{5}).$$

令 E 是 $f(x)$ 在 $\mathbb{Q}(\sqrt{5})$ 上的分裂域, 则 $E=\mathbb{Q}(\sqrt{5})(\sqrt[4]{5},\ \mathrm{i})$. 于是 $[E:\mathbb{Q}(\sqrt{5})]=4$, 因此 $\mathrm{Gal}(f(x),\mathbb{Q}(\sqrt{5}\ ))$ 是 4 阶群. 事实上, $\mathrm{Gal}(f(x),\mathbb{Q}(\sqrt{5}\ ))=\{\mathrm{id},\sigma,\tau,\gamma\}$, 其中

$$\sigma:\ \mathrm{i}\longmapsto \mathrm{i},\ \ \sqrt[4]{5}\longmapsto -\sqrt[4]{5};\ \ \tau:\mathrm{i}\longmapsto -\mathrm{i},\ \ \sqrt[4]{5}\longmapsto \sqrt[4]{5};\ \ \gamma:\mathrm{i}\longmapsto -\mathrm{i},\ \ \sqrt[4]{5}\longmapsto -\sqrt[4]{5}.$$

可见 $\mathrm{Gal}(f(x),\mathbb{Q}(\sqrt{5}\ ))=K_4$ (Klein 四元群).

(3) $f(x)=x^4-5\in\mathbb{Q}(\sqrt{5}\mathrm{i})[x]$ 是四次不可约多项式. $f(x)$ 在 $\mathbb{Q}(\sqrt{5}\mathrm{i})$ 上的分裂域 $\mathbb{Q}(\sqrt[4]{5},\mathrm{i})=\mathbb{Q}(\sqrt{5}\ \mathrm{i})(\sqrt[4]{5})$ 相对于 $\mathbb{Q}(\sqrt{5}\mathrm{i})$ 的维数是 4, 故 $\mathrm{Gal}(f(x),\mathbb{Q}(\sqrt{5}\ \mathrm{i}))$ 是 4 阶群, 这 4 个元为

$$\tau_1=\mathrm{id};\qquad \tau_2:\ \sqrt[4]{5}\longmapsto -\sqrt[4]{5};$$

$$\tau_3:\ \sqrt[4]{5}\longmapsto \sqrt[4]{5}\ \mathrm{i};\qquad \tau_4:\ \sqrt[4]{5}\longmapsto -\sqrt[4]{5}\ \mathrm{i}.$$

因 $\mathrm{i}=\dfrac{1}{5}\sqrt{5}\ \mathrm{i}(\sqrt[4]{5})^2$, $\dfrac{1}{5}\sqrt{5}\ \mathrm{i}\in\mathbb{Q}(\sqrt{5}\mathrm{i})$, 故 τ_2, τ_3, τ_4 均为 2 阶元, 从而 $\mathrm{Gal}(f(x),\mathbb{Q}(\sqrt{5}\ \mathrm{i}))=K_4$.

(4) 首先, $f(x)=x^4-10x^2+4$ 是 $\mathbb{Q}[x]$ 中的四次不可约多项式 (这可通过计算给出: 首先 $f(x)$ 没有有理根, 其次 $f(x)$ 不能分解成两个二次有理系数多项式的积). 由 $f(x)$ 诱导出的三次多项式为

$$g(x)=x^3+10x^2-16x-160=(x-4)(x+4)(x+10).$$

因此 $[\mathbb{Q}(4,-4,-10):\mathbb{Q}\ ]=1$. 由四次方程 Galois 群的一般结论知 $\mathrm{Gal}(f(x),\mathbb{Q})=K_4$. ■

4.2.7. 设 $n \geqslant 2$ 是正整数, 域 F 的特征为零或与 n 互素, ξ 是 n 次本原单位根, E 是 $f(x)=x^n-1$ 在 F 上的分裂域. 则

$$\mathrm{Gal}(f(x),F)=\begin{cases}(\mathbb{Z}_n)^*, & \xi\notin F,\\ \{1\}, & \xi\in F,\end{cases}$$

其中 $(\mathbb{Z}_n)^*$ 是 $\mathbb{Z}_n$ 的单位群.

证 首先 $E=F(\xi)$. 设 $\xi\notin F$. $\forall\,\sigma\in\mathrm{Gal}(E/F)$, $\sigma(\xi)=\xi^l$ $(1\leqslant l\leqslant n-1)$ 也是 n 次本原单位根, 故 $(l,n)=1$. 因 σ 由 l 唯一确定, 记 $\sigma=\sigma_l$, 于是 $\sigma_l\mapsto\bar{l}$ 就给出了群的单同态 $\mathrm{Gal}(f(x),F)\to(\mathbb{Z}_n)^*$.

对于任一 l, $(l,n)=1$, $1\leqslant l\leqslant n-1$, ξ 和 ξ^l 均是 n 次分圆多项式 $\Phi_n(x)$ 的根. 因 $\xi\notin F$, 故 $\Phi_n(x)$ 是 $F[x]$ 中不可约多项式, 从而 $\sigma_l(\xi)=\xi^l$, $(\sigma_l)|_F=\mathrm{id}$ 就给出了域同构 $F(\xi)\cong F(\xi^l)=F(\xi)$. 所以上述群的单同态也是群同构. ■

4.2.8. 设 $n\geqslant 2$ 是正整数, 域 F 的特征为零或与 n 互素, ξ 是 n 次本原单位根且 $\xi\in F$, E 是 $f(x)=x^n-a\in F[x]$ 在 F 上的分裂域. 则 $\mathrm{Gal}(f(x),F)$ 是循环群; 且当 $f(x)$ 在 F 上不可约时, $\mathrm{Gal}(f(x),F)$ 是 n 阶循环群. (注意与题 4.2.4 的区别.)

证 设 b 是 $f(x)$ 的一个根, 则 $b,b\xi,\cdots,b\xi^{n-1}$ 是 $f(x)$ 的全部根, $E=F(b)$. $\forall\,\sigma\in\mathrm{Gal}(E/F)$, $\sigma(b)=b\xi^i$, $0\leqslant i\leqslant n-1$. 因 σ 由 i 唯一确定, 记 $\sigma=\sigma_i$. 因为

$$\sigma_i\sigma_j(b)=\sigma_i(b\xi^j)=\sigma_i(b)\xi^j=b\xi^{i+j}=\sigma_{i+j}(b),$$

故 $\sigma_i\sigma_j=\sigma_{i+j}$, 其中下标模 n.

于是 $\sigma_i\mapsto\bar{i}$ 就给出了群的单同态 $\mathrm{Gal}(f(x),F)\to\mathbb{Z}_n$. 从而 $\mathrm{Gal}(f(x),F)$ 是循环群 $\mathbb{Z}_n$ 的子群, 故为循环群.

当 $f(x)$ 在 F 上不可约时, $[E:F]=n$. 因 E/F 是有限 Galois 扩张, 故 $|\mathrm{Gal}(f(x),F)|=[E:F]=n$. ■

4.2.9*. 设 p^n (p 为素数, $n\geqslant 1$) 次 Galois 扩张 E/F 的 Galois 群 $\mathrm{Gal}(E/F)$ 是 p^n 阶循环群, L 是 E/F 的中间域且 $[E:L]=p$. 若 $E=L(u)$, 则 $E=F(u)$.

证 设 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$. 因 E/L 是 p 次 Galois 扩张, 故 $\mathrm{Gal}(E/L)$ 是 p^n 阶循环群 $\langle\sigma\rangle$ 的 p 阶子群. 于是 $\mathrm{Gal}(E/L)=\langle\tau\rangle$, $\tau=\sigma^{p^{n-1}}$.

考虑多项式

$$f(x)=\prod_{0\leqslant i\leqslant p^n-1}(x-\sigma^i(u))\in E[x].$$

因为 $f^{\sigma^i}(x)=f(x)$, $0\leqslant i\leqslant p^n-1$, 所以 $f(x)$ 的系数均属于 $\mathrm{Inv}(\mathrm{Gal}(E/F))=F$. 下证 $f(x)$ 无重根.

令 H 是 $\mathrm{Gal}(E/F)$ 中保持 u 不动的自同构作成的子群, 则 $|H|=1$, 从而 $f(x)$ 无重根. 否则, H 包含 $\mathrm{Gal}(E/F)$ 的最小子群 $\mathrm{Gal}(E/L)$, 于是

$$u \in \mathrm{Inv}(H) \subseteq \mathrm{Inv}(\mathrm{Gal}(E/L)) = L,$$

从而得到矛盾 $E=L(u)=L$.

注意 $f(x)$ 在 F 上的分裂域为 $K=F(\sigma^i(u),\ 0 \leqslant i \leqslant p^n-1)$, 则 $K=E$. 否则, $\mathrm{Gal}(E/K)$ 是阶大于 1 的 $\mathrm{Gal}(E/F)$ 的子群, 从而包含 $\mathrm{Gal}(E/L)$, 于是 $K \subseteq L$. 但 $u \in K$, 故再次得到矛盾 $u \in L$.

于是, 无重根多项式 $f(x)$ 在 F 上的 Galois 群 $\mathrm{Gal}(K/F)=\mathrm{Gal}(E/F)=\langle\sigma\rangle$ 是 $f(x)$ 根的可迁置换群, 因此 $f(x)$ 在 F 上不可约. 于是 $[F(u):F]=p^n$, 从而 $E=F(u)$. ■

用类似的方法可以证明下面更一般的结果.

4.2.10*. 设 E/F 是有限次 Galois 扩张, 其 Galois 群 $\mathrm{Gal}(E/F)$ 含有最小子群 A, $L=\mathrm{Inv}(A)$. 若 $E=L(u)$, 则 $E=F(u)$.

4.2.11. 任一有限群均是某个域上可分多项式的 Galois 群.

证 任一有限群 G 均是某个对称群 S_n 的子群. 而 $S_n=\mathrm{Gal}(E/K)$, 其中 $E=F(x_1,\cdots,x_n)$, $K=F(t_1,\cdots,t_n)$, 这里 $x_1,\cdots,x_n$ 是域 F 上独立的代数无关元, $t_1,\cdots,t_n$ 是 $x_1,\cdots,x_n$ 的初等对称多项式. 注意 E/K 是有限 Galois 扩域. 由 Galois 理论的基本定理知, 存在 K 和 E 的中间域 L 使得 $G=\mathrm{Gal}(E/L)$. 因为 E/L 也是有限 Galois 扩域, 故 E 是 L 上某个可分多项式 $f(x)$ 在 L 上的分裂域, 从而 $G=\mathrm{Gal}(E/L)=\mathrm{Gal}(f(x),L)$. ■

注 任一有限群是否是某个事先给定域上可分多项式的 Galois 群? 这是一个十分困难的问题. 例如, 任一有限群是否是 $\mathbb{Q}$ 上某个多项式的 Galois 群? 这是迄今为止尚未解决的公开问题.

§3　方程的根式可解性

知识要点:

域 F 的单扩张 $E=F(d)$ 称为根式扩张, 如果存在正整数 n 使得 $d^n \in F$.

设 $f(x) \in F[x]$ 是正次数多项式. 称方程 $f(x)=0$ 在 F 上根式可解, 如果存在域扩张链

$$F=F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{r+1}=K,$$

使得 F_{i+1}/F_i 均为根式扩张, $1 \leqslant i \leqslant r$, 且 $E \subseteq K$, 其中 E 是 $f(x)$ 在 F 上的分裂域.

Galois 大定理: 设 $f(x)$ 是特征零域 F 上正次数多项式, 则 $f(x)=0$ 在 F 上根式可解当且仅当 $\mathrm{Gal}(f(x),F)$ 是可解群.

下面以习题的形式给出这个重要定理的证明.

4.3.1*. 设 p 次 Galois 扩张 E/F 的 Galois 群 $\mathrm{Gal}(E/F)$ 是 p 阶循环群 (p 为素数), 且 F 含有 p 次本原单位根 ξ. 则存在 $d\in E$ 使得 $E=F(d)$, $d^p\in F$. 故 E/F 是根式扩张.

证 因 $[E:F]=p$, 故 $E=F(c)$, 其中 c 是 E 中不属于 F 的任一元. 设 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$, $\sigma^p=1$. 考虑 Lagrange 预解式

$$d_i=c+\sigma(c)\xi^i+\sigma^2(c)\xi^{2i}+\cdots+\sigma^{p-1}(c)\xi^{(p-1)i}\in E.$$

因 $\xi\in F$, 故 $\sigma(\xi)=\xi$. 于是 $\sigma(d_i)=\sigma(c)+\sigma^2(c)\xi^i+\cdots+\sigma^{p-1}(c)\xi^{(p-2)i}+c\xi^{(p-1)i}=\xi^{-i}d_i$. 从而

$$\sigma(d_i^p)=(\sigma(d_i))^p=(\xi^{-i}d_i)^p=d_i^p.$$

因 E/F 是有限 Galois 扩张, 故 $d_i^p\in\mathrm{Inv}(\langle\sigma\rangle)=F$, $1\leqslant i\leqslant p$.

考虑 p 个变元 p 个方程的线性方程组

$$x_1+\xi^i x_2+\xi^{2i}x_3+\cdots+\xi^{(p-1)i}x_p=d_i,\quad 1\leqslant i\leqslant p,$$

其系数行列式是 $1,\xi,\cdots,\xi^{p-1}$ 的 Vandermonde 行列式; $(c,\sigma(c),\cdots,\sigma^{p-1}(c))$ 是其唯一解. 因 $c,\sigma(c),\cdots,\sigma^{p-1}(c)$ 是 $d_1,\cdots,d_p$ 的 F- 线性组合, $c\notin F$, 故存在 $d_j\notin F$. 取 $d=d_j$, 则 $E=F(d)$, $d^p\in F$. ■

4.3.2*. 设域 F 的特征为零, E 是 F 上正次数多项式 $f(x)$ 在 F 上的分裂域. 若 $\mathrm{Gal}(E/F)$ 是可解群, 则 $f(x)=0$ 在 F 上根式可解.

证 令 $n=[E:F]=|\mathrm{Gal}(E/F)|$, $\xi=\xi_n$ 是 n 次本原单位根, $F_2=F(\xi)$, $K=E(\xi)$. 则 K 是 $f(x)$ 在 F_2 上的分裂域, 故 K/F_2 是有限 Galois 扩张.

设 $E=F(\alpha_1,\cdots,\alpha_m)$, 其中 $\alpha_1,\cdots,\alpha_m$ 是 $f(x)$ 的全部根. 则 $\mathrm{Gal}(F(\xi)(\alpha_1,\cdots,\alpha_m)/F(\xi))$ 可以自然地看成 $\mathrm{Gal}(F(\alpha_1,\cdots,\alpha_m)/F)$ 的子群. 即 $\mathrm{Gal}(K/F_2)$ 是可解群 $\mathrm{Gal}(E/F)$ 的子群, 从而也是可解群. 故有次正规群列 (未必是正规群列)

$$\mathrm{Gal}(K/F_2)=H_2\rhd H_3\rhd\cdots\rhd H_{r+1}=\{1\},$$

使得 H_i/H_{i+1} 均为 p_i 阶循环群.

由 Galois 理论基本定理得到域的扩张链

$$F_2\subseteq F_3\subseteq\cdots\subseteq F_{r+1}=K,$$

其中 $F_i = \mathrm{Inv}(H_i)$. 因为 K/F_i 是有限 Galois 扩张, $H_i = \mathrm{Gal}(K/F_i)$, H_{i+1} 是 H_i 的正规子群. 对于 K/F_i 用 Galois 理论基本定理知 F_{i+1}/F_i 是正规扩域 (从而是有限 Galois 扩张且 $[F_{i+1}:F_i] = |\mathrm{Gal}(F_{i+1}/F_i)|$), 且

$$\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}.$$

因 $\xi \in F_2$, $p_i \mid |\mathrm{Gal}(K/F_2)| \mid n$, 故 F_i 包含 p_i 次本原单位根. 因此由题 4.3.1 知 F_{i+1}/F_i 是根式扩张, $2 \leqslant i \leqslant r$. 从而有根式扩张链

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{r+1} = K,$$

使得 $E \subseteq K = E(\xi)$, 即 $f(x) = 0$ 在 F 上根式可解. ■

4.3.3*. 设 F 是任意特征的域, E/F 是有限可分扩张. 若 E/F 有根式扩张链, 则存在 E 的有限扩域 N, 使得 N/F 是有限正规扩张, 且 N/F 也有根式扩张链.

证 设 $E = F(\alpha_1, \cdots, \alpha_m)$, $f_i(x)$ 是 α_i 在 F 上的极小多项式, 则 $f_i(x)$ 无重根. 令 N 是 $f_1(x)\cdots f_m(x)$ 在 F 上的分裂域, 则 N/F 是有限 Galois 扩张.

设 E/F 有根式扩张链

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{r+1} = E,$$

使得 $F_{i+1} = F_i(d_i)$, $d_i^{n_i} \in F_i$, $1 \leqslant i \leqslant r$. 则 $E = F(d_1, \cdots, d_r)$. 设 $\mathrm{Gal}(N/F) = \{1 = \sigma_1, \sigma_n\}$, $n = [N:F]$. 因为 N 是包含 E 的 F 的最小正规扩域, 故 (由题 3.7.6 可知)

$$N = F(d_1, \cdots, d_r, \sigma_2(d_1), \cdots, \sigma_2(d_r), \cdots, \sigma_n(d_1), \cdots, \sigma_n(d_r)).$$

考虑如下域扩张链

$$\begin{aligned}
&F \subseteq F(d_1) \subseteq F(d_1, \sigma_2(d_1)) \subseteq \cdots \subseteq F(d_1, \sigma_2(d_1), \cdots, \sigma_n(d_1)) \\
&\subseteq F(d_1, \sigma_2(d_1), \cdots, \sigma_n(d_1), d_2) \subseteq \cdots \\
&\subseteq F(d_1, \sigma_2(d_1), \cdots, \sigma_n(d_1), d_2, \sigma_2(d_2), \cdots, \sigma_n(d_2)) \\
&\subseteq \cdots \subseteq F(d_1, \cdots, \sigma_n(d_1), d_2, \cdots, \sigma_n(d_2), \cdots, d_r, \cdots, \sigma_{n-1}(d_r)) \subseteq N.
\end{aligned}$$

不难看出这是根式扩张链. ■

4.3.4*. 设域 F 的特征为零, E 是 F 上正次数多项式 $f(x)$ 在 F 上的分裂域. 若 $f(x) = 0$ 在 F 上根式可解, 则 $\mathrm{Gal}(E/F)$ 是可解群.

证 由定义存在域扩张链

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{r+1} = K,$$

使得 $F_{i+1} = F_i(d_i)$, $d_i^{n_i} \in F_i$, $1 \leqslant i \leqslant r$, 且 $E \subseteq K$. 由题 4.3.3 不妨设 K/F 是正规扩张. 令 n 是 $n_1, \cdots, n_r$ 的公倍数, ξ 是 n 次本原单位根. 则 $K(\xi)/F$ 是有限 Galois 扩张, 且有域扩张链

$$F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_{r+1} = K(\xi),$$

其中 $E_i = F_i(\xi)$, $1 \leqslant i \leqslant r+1$. 将 $\mathrm{Gal}(K(\xi)/-)$ 作用在这个域扩张链上得到群的降链

$$\mathrm{Gal}(K(\xi)/F) \supseteq \mathrm{Gal}(K(\xi)/E_1) \supseteq \mathrm{Gal}(K(\xi)/E_2) \supseteq \cdots \supseteq \{1\}.$$

注意 $E_1/F = F(\xi)/F$ 是正规扩域. 又因为

$$E_{i+1} = F_{i+1}(\xi) = F_i(d_i)(\xi) = F_i(\xi)(d_i) = E_i(d_i),\ d_i^{n_i} \in E_i,\ 1 \leqslant i \leqslant r,$$

E_i 包含 n_i 次本原单位根, 故 E_{i+1}/E_i 均为正规扩域, $0 \leqslant i \leqslant r$. 因为 $K(\xi)/F$ 是有限 Galois 扩张, 故 $K(\xi)/E_i$ 均是有限 Galois 扩域. 对 $K(\xi)/E_i$ 用 Galois 理论基本定理知 $\mathrm{Gal}(K(\xi)/E_{i+1})$ 是 $\mathrm{Gal}(K(\xi)/E_i)$ 的正规子群, $0 \leqslant i \leqslant r$. 所以上述群的降链还是 $\mathrm{Gal}(K(\xi)/F)$ 的次正规群列, 且由 Galois 理论基本定理知

$$\mathrm{Gal}(K(\xi)/E_i)/\mathrm{Gal}(K(\xi)/E_{i+1}) \cong \mathrm{Gal}(E_{i+1}/E_i),\ 0 \leqslant i \leqslant r.$$

由题 4.2.7 知 $\mathrm{Gal}(E_1/F)$ 是 Abel 群; 而由题 4.2.8 知 $\mathrm{Gal}(E_{i+1}/E_i)$ 也都是 Abel 群, $1 \leqslant i \leqslant r$. 从而由可解群的等价刻画知 $\mathrm{Gal}(K(\xi)/F)$ 是可解群.

因为 $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K(\xi)/F)/\mathrm{Gal}(K(\xi)/K)$, 故 $\mathrm{Gal}(K/F)$ 是可解群. 而 $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$, 故 $\mathrm{Gal}(E/F)$ 也是可解群. ■

至此完成 Galois 大定理的证明.

参 考 文 献

[FLZZ] 冯克勤, 李尚志, 查建国, 章璞. 近世代数引论. 合肥: 中国科学技术大学出版社, 1988 (第 1 版), 2002 (第 2 版), 2009 (第 3 版)

[FY] 冯克勤, 余红兵. 整数与多项式. 北京: 高等教育出版社, 施普林格出版社, 1999

[FZL] 冯克勤, 章璞, 李尚志. 群与代数表示引论. 第 2 版. 合肥: 中国科学技术大学出版社, 2006

[H] 华罗庚. 数论导引. 北京: 科学出版社, 1979

[J] Jacobson N. Basic Algebra (I), (II). W. H. Freeman and Company, 1974, 1980

[L] 刘绍学. 近世代数基础. 北京: 高等教育出版社, 1999

[ND] 聂灵沼, 丁石孙. 代数学引论. 第二版. 北京: 高等教育出版社, 2000

[V] Van der Waerden B L. 代数学 (I), (II). 丁石孙, 曾肯成, 郝炳新译. 万哲先校. 北京: 科学出版社, 1955, 1976

[W] 万哲先. 代数导引. 北京: 科学出版社, 2004

[WH] Weyl H.. Symmetry. Princeton University Press, 1952 (中译本: 冯承天, 陆继宗译. 上海: 上海科学技术教育出版社, 2002)

[X] 谢邦杰. 抽象代数学. 上海: 上海科学技术出版社, 1982

[Z] 张禾瑞. 近世代数基础. 第二版. 北京: 高等教育出版社, 1978